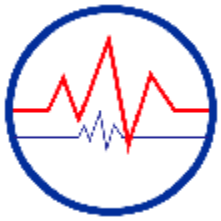
Baseline™ IDS



基准入侵检测系统
使用手册

User Manual

Version 5.0

5

版权声明

北京杰马创新科技有限责任公司
Beijing G&M Innovation Co.,LTD
地址：北京市丰台区草桥欣园一区 **2#1802**
电话：（**010**）**87583031**
网址：http://www.gminnova.com.cn

基准入侵检测系统用户使用手册

Baseline IDS
User Manual

版权声明
北京杰马创新科技有限责任公司©2004 版权所有，保留一切权力。
未经北京杰马创新科技有限责任公司书面同意不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。本文档中的信息归北京杰马创新科技有限责任公司所有并受中国知识产权法和国际公约的保护。

信息更新
本文档及其相关计算机软件程序（以下文中称为“文档”）仅用于为最终用户提供信息，并且随时可由北京杰马创新科技有限责任公司（下称“杰马”）更改或撤回。

信息反馈
如有任何宝贵意见，请反馈：
信箱：北京市丰台区草桥欣园一区 **2#1802**
电话：010-87583031

免责条款
根据适用法律的许可范围，杰马公司按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，杰马公司都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使杰马公司明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。
本文档中所有引用产品的使用及本文档均受最终用户可适用的特许协议约束。

出版时间
本文档由北京杰马创新科技有限责任公司2004年10月制作出版。

==========

软件产品许可协议

本产品受著作权法及国际条约条款和其它知识产权法及条约的保护。本产品提供使用许可协议，禁止出售。

权利和限制说明。

1、不得对本产品进行反向工程、反编译或反汇编，但如相关法律明文禁止上述限制，则不在此限；

2、本产品是被当成一个单一产品而被授予许可协议，拷贝或转交必须包含本产品的全部；

3、不得出租或租赁本产品和授权许可证；

4、您可以永久转让您在本《协议》下的所有权利，条件是您不得保留副本，并将本“软件产品”全部转让（包括所有组成部分：软件、资料文档、相关媒介以及印刷材料），并且受让人须接受本协议的各项条款。如本产品属于更新版本，则任何转让必须包括本产品以前的所有版本。

5、如您未遵守本《协议》的各项条件，北京杰马创新科技有限责任公司有权终止本协议。如发生此种情况，则您必须销毁本产品及其各部分的所有副本。

==========

本协议以《中华人民共和国著作权法》,《软件保护条例》和《国际版权公约》为依据。

北京杰马创新科技有限责任公司保留对本协议的解释权。

目 录

1. 序言 1
2. Baseline IDS 概述 3
2.1 安全困惑与需求 3
2.2 网络安全与 P2DR2 模型 4
2.3 关于基准入侵检测系统 Baseline IDS 5
2.4 Baseline IDS 功能 6
2.5 Baseline IDS 特点 8
3. Baseline IDS 体系结构 11
3.1 Baseline IDS 体系结构 11
3.2 Baseline IDS 模块结构 12
3.3 Baseline IDS 工作方式 14
3.4 Baseline IDS 工作原理 15
4. Baseline IDS 性能指标 17
4.1 Baseline IDS 5.0 综合性能 17
4.2 集中安全管理中心（IDS Console） 18
4.3 分布式探针（IDS Sensor） 19
5. Baseline IDS 运行环境 23
5.1 Baseline IDS 的物理介质 23
5.2 Baseline IDS 运行环境 24
5.3 集中安全管理中心的运行环境 24
5.4 分布式探针的运行环境 25
6. 功能介绍 27
6.1 系统登录 27
6.2 锁定系统与系统解锁 28
6.2.1 锁定系统 29
6.2.2 系统解锁 29
6.3 注销用户 30
6.4 退出系统 31
7. 系统维护 33
7.1 功能介绍 33
7.2 系统授权 33
7.3 配置参数 35
7.3.1 进入工作参数配置窗体 35
7.3.2 系统参数 36
7.3.3 SMS 告警 37
7.3.4 Scan 告警 38
7.3.5 Email 告警 39
7.4 用户管理 40
7.4.1 用户的三级权限 40
7.4.2 进入用户管理 40
7.4.3 用户管理的功能描述 42
7.5 数据库管理 43
7.5.1 进入数据库管理界面 43
7.5.2 数据库管理的功能描述 44
8. 系统视图 49
8.1 功能介绍 49
8.1.1 各部分功能的描述 50
8.2 显示、隐藏树列表 52
8.3 显示、隐藏信息栏 53
9. 探针管理 55
9.1 功能介绍 55
9.2 添加探针 55
9.3 连接探针 58
9.4 断开探针 59
9.5 探针属性 59

9.6 修改探针 60
9.7 删除探针 64
9.8 探针日志 64
9.9 查找探针 65
9.10 升级探针 66
10. 策略管理 67
10.1 功能介绍 67
10.2 策略管理 67
10.2.1 接收策略 67
10.2.2 新建策略 69
10.2.3 编辑和查看策略 72
10.2.4 上传和下载策略 72
10.2.5 删除策略 73
10.3 规则过滤和地址绑定 73
10.3.1 进入地址过滤 73
10.3.2 规则过滤和地址绑定的功能描述 74
10.4 禁用黑名单 77
10.4.1 添加功能 78
10.4.2 删除功能 78
11. 系统审计 79
11.1 功能介绍 79
11.2 系统告警报告 79
11.3 用户操作审计 81
11.4 安全趋势分析 82
11.5 告警数据审计 83
11.6 网络事件回放 86
12. 系统帮助 87
12.1 功能介绍 87
12.2 进入系统帮助 87
12.3 网上 IDS 系统 88
12.4 系统在线升级 88
12.5 系统版本信息 88
13. 疑难解答 FAQs 89

图表

图表 1 安全威胁与需求 3
图表 2P2DR2 安全管理模型 4
图表 3 入侵检测系统的构成 12
图表 4 分布式探针的模块构成 12
图表 5 集中安全管理中心的模块构成 13
图表 6 分布式检测-集中式安全管理方式 14
图表 7 入侵检测预警预响应系统布控示例 15
图表 8 入侵检测系统工作原理 16
图表 9 入侵检测系统快捷方式图标 33
图表 10 登录系统身份验证 34
图表 11 入侵检测系统界面 35
图表 12 锁定系统子菜单 35
图表 13 系统处于锁定状态时的显示形式 35
图表 14 系统解锁菜单 36
图表 15 用户重新登录系统身份验证界面 36
图表 16 注销用户子菜单 37
图表 17 退出系统子菜单 37
图表 18 身份认证失败 37
图表 19 系统授权子菜单 33
图表 20 许可证选择 34
图表 21 许可证信息 34
图表 22 配置参数子菜单 35
图表 23 安全管理中心工作参数配置 36
图表 24SMS 告警参数设置 37
图表 25 扫描确认 38
图表 26EMAIL 告警参数设置 39
图表 27 用户管理子菜单 40
图表 28 进入用户管理 41
图表 29 添加用户 42
图表 30 更改密码 42
图表 31 删除用户确认 43
图表 32 数据库管理子菜单 43
图表 33 数据库管理界面 44
图表 34 查看数据库表 44
图表 35 备份数据库表 45
图表 36 数据库备份完成 45
图表 37 导入数据库表 46
图表 38 数据库表导入完成 46
图表 39 清空数据库表 47
图表 40 数据库清空确认 47
图表 41 数据库表清空完成 47
图表 42 界面划分图 49
图表 43 列表视弹出式菜单 50
图表 44 低风险视图 50
图表 45 流量监测视图 51
图表 46 拓扑结构视图 51
图表 47 系统操作命令列表视图 52
图表 48 状态栏视图 52
图表 49 树列表子菜单 52
图表 50 工具栏树列表视图 52
图表 51 隐藏树列表视图后的系统显示状态 53

图表 52 添加探针子菜单.....55
图表 53 添加探针第一步.....56
图表 54 添加探针第二步.....56
图表 55 添加探针第三步.....57
图表 56 连接探针子菜单.....58
图表 57 探针联接成功时树视图状态.....58
图表 58 探针联接成功时信息栏状态.....58
图表 59 断开探针子菜单.....61
图表 60 树视图中的断开探针子菜单.....59
图表 61 探针属性弹出式子菜单.....59
图表 62 探针属性对话框.....60
图表 63 修改探针子菜单.....60
图表 64 树视图中的修改探针子菜单.....61
图表 65 修改探针第一步.....61
图表 66 修改探针第二步.....62
图表 67 添加探针第三步.....62
图表 68 删除探针子菜单.....64
图表 69 删除探针确认.....64
图表 70 探针日志子菜单.....64
图表 71 探针日志确认.....65
图表 72 日志显示在写字板上.....65
图表 73 查找探针子菜单.....65
图表 74 升级探针子菜单.....66
图表 75 策略管理子菜单.....67
图表 76 策略管理界面.....68
图表 77 策略成功接收提示.....68
图表 78 探针策略编辑器.....69
图表 79 新建策略.....69
图表 80 网络基本输入/输出系统攻击.....70
图表 81 新增事件的相关信息输入.....70
图表 82 事件规则定义.....71
图表 83 探针下拉菜单.....72
图表 84 策略上传确认对话框.....72
图表 85 上载策略选择对话框.....73
图表 86 地址过滤子菜单.....73
图表 87 规则过滤和地址绑定.....74
图表 88 设置过滤 IP 地址.....74
图表 89 选中删除 IP 项.....75
图表 90 绑定 MAC 地址和 IP 地址窗体.....75
图表 91 选中删除项.....76
图表 92 禁用黑名单主界面.....77
图表 93 添加黑名单.....78
图表 94 系统审计报告子菜单.....79
图表 95 报告显示界面.....79
图表 96 报表查询.....80
图表 97 源地址明细报表.....80
图表 98 用户操作审计子菜单.....81
图表 99 用户操作审计界面.....81
图表 100 设置查询条件.....82
图表 101 安全趋势分析子菜单.....82
图表 102 设置条件.....82
图表 103 显示趋势分析成功.....83
图表 104 一个趋势分析实例.....83

图表 105 告警数据审计子菜单 83
图表 106 数据审计主界面 84
图表 107 定制窗口界面 84
图表 108 数据查询参数 85
图表 109 导出数据审计 85
图表 110 网络事件回放子菜单 86
图表 111 网络事件回放 86
图表 112 系统帮助菜单 87
图表 113 系统帮助 87

1. 序言

编写目的

《基准入侵检测系统 IDS V5.0 使用手册》用于指导怎样使用杰马公司的产品 IDS V5.0，它适合如下的读者群体：

（1） 安装、配置基准入侵检测系统 IDS V5.0 的用户读者；

（2） 检测、评估基准入侵检测系统 IDS V5.0 的测试机构的技术人员和专家；

（3） 希望使用基准入侵检测系统 IDS 5.0 实现企业信息与网络系统安全策略的组织、机构和企业的技术人员、专家和决策者；

（4） 希望深入了解基准入侵检测系统的读者群体；

项目背景

产品中文名称：基准入侵检测系统

产品英文名称：Baseline IDS

产品出处：北京杰马创新科技有限责任公司

产品开发者：北京杰马创新科技有限责任公司 BIDS 小组

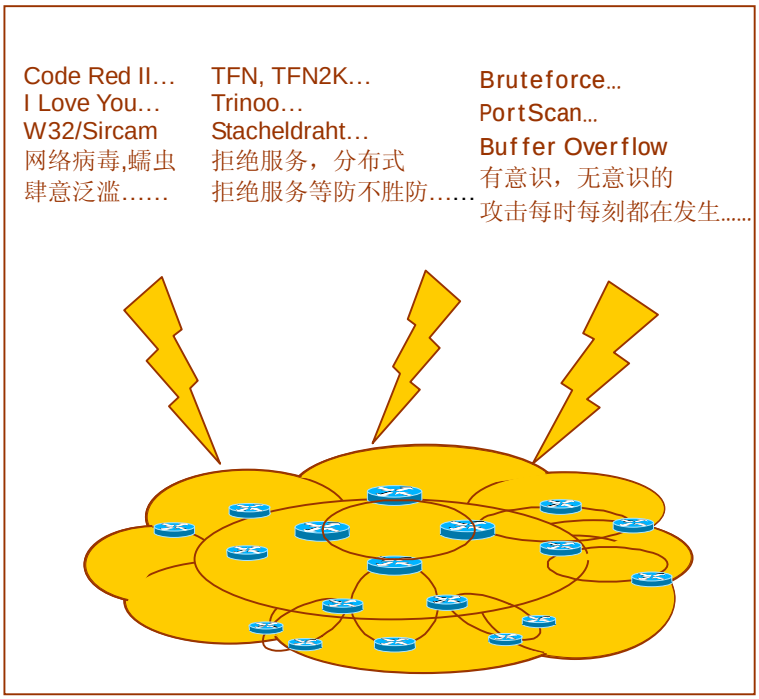
2. Baseline IDS 概述

基准入侵检测系统 Baseline IDS 作为一种基于网络的入侵检测系统，它在信息网络安全中到底发挥什么样的作用？在网络系统的定位如何？本章进行详细介绍，主要介绍的内容有：

- 安全困惑与需求
- 关于入侵检测系统？
- 它在信息网络安全中的定位，它有那些功能？
- 和其他系统相比，它具备那些明显的优势和特点？

2.1 安全困惑与需求

的确，我们人类发明了计算机，构建了网络，计算机和网络在大大推动社会发展进程的同时，又给我们带来了无穷无尽的困扰。我们的生活越来越依赖计算机和网络，我们开始提心吊胆，因为工作和生活开始失去切实的安全感，病毒、黑客、攻击等等是我们无形的敌人，它们窥探着我们的生活空间，压抑着我们自由的欲望。在它们隐藏着恶意的情况下，我们只有一个深切的呼唤：安全！安全！只有拥有实在的安全感，我们在自己的空间里才可能自由地舒展。如图 1 所示：

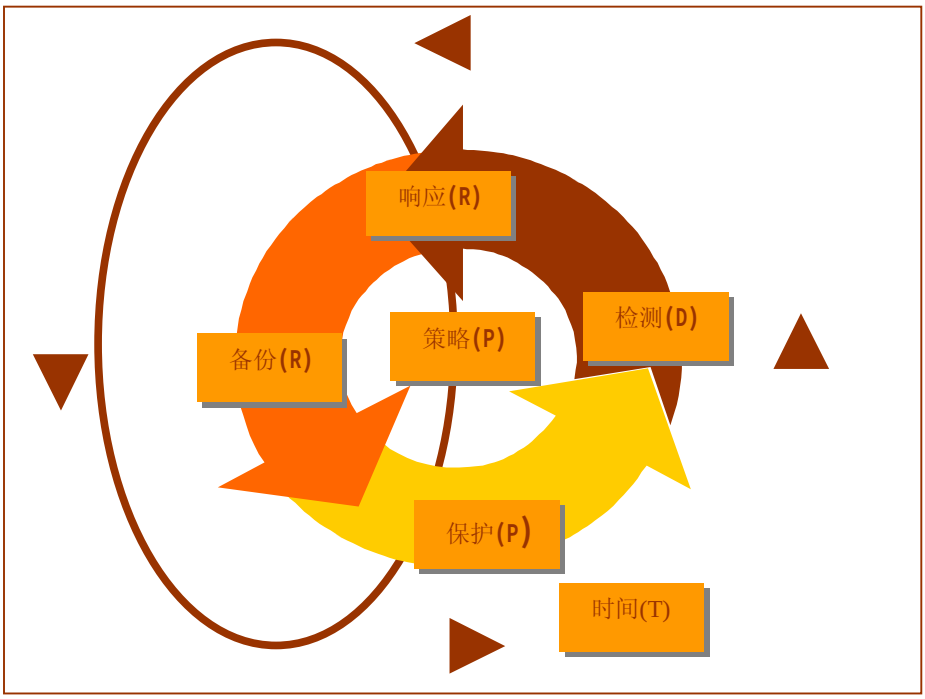


图表 1 安全威胁与需求

2.2 网络安全与P2DR2模型

在不足一代人的时间内，信息革命和计算机以惊人的速度渗透到人类社会各个层面，人类已经跨入了信息化、网络化时代。信息与网络正以前所未有的方式悄然改变着人们日常生活的组织方式、经济的运作方式以至国家安全的保障方式。

随着社会发展，信息，已成为最能代表综合国力的战略资源。伴随而来的信息安全问题也在全球范围内突现出来，能否有效地保护信息资源，保护信息化进程健康、有序、可持续发展，直接关系到国家安危，关系到民族兴亡，是国家、民族的头等大事。没有信息安全，就没有真正意义上的政治安全，就没有稳固的经济安全和军事安全，更没有完整意义上的国家安全。



图表 2P2DR2 安全管理模型

信息与网络系统安全理论和方法学正在经历一个重大的变革。由于传统的计算机安全理论不能适应动态变化的、多维互联网络环境，可适应网络安全理论体系逐渐形成。目前普遍崇尚可适应的动态网络安全理论来确保网络系统的安全。这种理论就是基于 P2DR2 安全模型的动态信息安全理论。如图 2 所示：

P2DR2 模型是在整体的网络系统安全策略（Policy）的控制和指导下，综合运用诸如安全操作系统、防火墙、身份认证、访问控制、加密等安全防护措施和手段(Protection)保证网络系统具有一定的安全基础。同时，为保证安全防护措施和手段正确地按照安全策略的要求工作，利用入侵监控系统适时地监控网络事件，确保网络安全，采用弱点漏洞分析和评估工具定期对网络的安全状况进行评估和分析，以期网络始终保持相对的安全状态（Detection）。对网络入侵行为和动态的网络弱点漏洞，不正确的系统配置和使用进行响应（Response）和培训。同时定期对系统重要资源进行备份（Recovery）,最大限度地减少网络安全事件带来的风险和损失。

2.3 关于基准入侵检测系统Baseline IDS

当越来越多的公司将其核心业务向互联网转移的时候，网络安全作为一个无法回避的问题呈现在人们面前。传统上，公司一般采用防火墙作为安全的第一道防线。而随着攻击者知识的日趋成熟，攻击工具与手法的日趋复杂多样，单纯的防火墙策略已经无法满足对安全高度敏感的部门的需要，网络的防卫必须采用一种纵深的、多样的手段。与此同时，当今的网络环境也变得越来越复杂，各式各样的复杂的设备，需要不断升级、补漏的系统使得网络管理员的工作不断加重，不经意的疏忽便有可能造成安全的重大隐患。在这种环境下，入侵检测系统成为了安全市场上新的热点，不仅愈来愈多的受到人们的关注，而且已经开始在各种不同的环境中发挥其关键作用。

入侵检测作为 P2DR2 安全管理模型中很重要的一个安全管理环节—Detection，是对防火墙等防护产品的一个安全功能的扩展和安全功能的补充。

“网络入侵”（Intrusion）是个广义的概念，不仅包括被发起攻击的人（如恶意的黑客）取得超出合法范围的系统控制权，也包括收集漏洞信息，造成拒绝访问（Denial of Service）等对计算机系统造成危害的行为。检测（Intrusion Detection），是对入侵行为的发觉。它通过对计算机网络或计算机系统中得若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。预警是对网络行为分析后，对网络可能受到的威胁发出攻击朕兆预报，提请用户或系统管理员注意。响应是对违规操作，网络入侵行为等进行相应的处理措施，如报警，记录日志，阻断网络连接等等。分布式（Distributed）是指系统能同时并行地支持多个探针（Probes 或 Sensors），并行地管理和保护多个网段或子网。

入侵检测系统是实时网络自动违规识别和响应系统，是一种实时的、自动的网络入侵与违规行为识别、网络攻击情报预警和对入侵行为与征兆的响应系统。该系统采用分布式监控和集中式管理的方法来实行对企业级的网络系统进行全面的入侵行为监测、，它是一种分布式的集群系统。它位于被保护的内部网络和不安全的外部网络之间，通过实时截获网络数据流，寻找网络违规模式和未授权的网络访问尝试。当发现网络违规模式和未授权的网络访问时，网络信息安全检测预警系统能够根据系统安全策略做出反应，包括实时报警，事件登录，自动阻断通信连接或执行用户自定义的安全策略等。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须可以将得到的数据进行分析，并得出有用的结果。一个合格的入侵检测系统能大大的简化管理员的工作，保证网络安全的运行。

2.4 Baseline IDS功能

入侵检测系统是集检测、预警、响应、审计、报告和分布式集中管理功能于一体的网络安全产品，它的强大功能主要表现在：

- **强大的攻击检测能力(Detection)**
  - IDS 检测基于攻击特征规则数据库

    基准 IDS 内置已知网络攻击特征/模式数据库，能够根据网络数据流和网络通讯会话轨迹，智能地与网络攻击模式进行匹配。对确认为攻击的行为，系统进行阻断会话、制止攻击、日志记录、系统告警或者进行反攻击等响应。目前基准 IDS 能够识别的攻击特征/模式的数量为 1312 个，是目前在用的 IDS 中，支持数目最多的系统。
  - 基准 IDS 的检测基于多种分析、识别模式

    系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。取测量属性的平均值作为阀值，用来与网络、系统的行为进行比较，任何观察值在偏离统计阀值一定范围之时，就认为是入侵行为。主要分析方法有：
    - 基于模式、表达式或字符串的匹配
    - 基于行为频次、频率和阀值的分析
    - 基于会话的相关性的低级安全事件的识别
    - 基于规律统计的非常规现象的检测
    - 基于知识的智能系统识别
  - 基准 IDS 的检测基于自定义规则

    基准 IDS 不仅能提供缺省的分布式探针模板，而且它允许用户根据系统规则生成用户模板。同时，它还以某种方式支持用户定义的用户网络安全事件，提高了系统攻击特征规则数据库的扩充能力。
- **强大的违规操作预警能力(Alert)**

  基准 IDS 能够对系统在一定时间段内的安全状况进行趋势分析，并对有入侵倾向的行为提前告警，使安全风险降到最小，体现了强大的预警功能。
- **强大的响应能力（Response）**

  基准 IDS 对检测到的入侵行为（或称*安全事件*）根据安全策略的要求，采取适当的响应方式进行反应。系统提供七种响应方式：
  - 事件回放能力（RePlay）

    基准 IDS 能将所发生的网络安全事件实时的显示在集中安全管理中心上，并对关键的会话进行回放。
  - 事件报警能力(Alert)

    基准 IDS 能够根据所发生的网络安全事件的不同级别发出不同的报警声音。

- 事件日志能力(LogDB)

  基准 IDS 能够自动响应网络安全事件，并将网络事件发生的日期和时间，事件的源与目的 IP 地址等有关攻击信息记录到日志数据库中，留作审计分析和备查。

- 邮件通知能力(E-Mail)

  基准 IDS 能将攻击事件通过 E-mail 发送给管理员设置的信箱中。

- 扫描器策略联动(Scan)

  基准 IDS 能将报警事件相关策略发送给弱点漏洞分析系统扫描确认。

- 发送 SNMP Trap 信息能力（SNMP Trap）

  基准 IDS 能将攻击事件给网管中心发送标准网管信息，支持 SNMP v1、v1.7、v2.0.

- 实时通讯连接阻断和攻击制止能力(RstSession)

  基准 IDS 能够根据用户安全策略的定义对攻击行为和违规行为进行会话终止响应，制止攻击事件的延续，最大限度地保证网络系统的安全。

  此外，系统还提供了与其他网络设备或安全系统协同工作的响应方式，称为“联动响应”。

- 支持与防火墙的联动响应能力(ResetFW)

  设置防火墙的过滤规则，对入侵行为的源地址进行封堵。

- 支持与路由器的联动响应能力(ReLoadRACL)

  设置路由器的 ACL，对入侵行为的源地址进行过滤。

n 日志审计分析的能力(Audit)

基准 IDS 提供智能化的日志审计分析能力，灵活地支持用户要求的多种安全事件的审计、分析、查询与检索能力。确保用户及时、准确地掌握网络行为的状况。

n 生成报告的能力(Report)

基准 IDS 能从繁杂的网络报警和日志信息中生成反映网络安全问题的定性及定量统计报表，如：各种类型的报警事件占报警总数百分比分析报告、涉及报警事件的主机分析报告、网络攻击源主机及被攻击的目标主机分析报告、违规源主机和目的主机分析报告等等。通过这些报告网络安全管理人员可对网络的安全状况有一个基本的了解。

n 入侵检测与集中安全管理功能(Managment)

基准 IDS 能够支持多个分布式探针，对多个网段同时进行入侵检测，支持多达 50 个 Sensors，实现分布式集中管理。

正因为具备上述强大功能，IDS 能实现安全路由器、信息加密系统、授权与身份认证系统防火墙等

安全产品所不能实现的防护能力，使之成为国内外新一代的网络安全产品。

2.5 Baseline IDS特点

基准入侵检测系统是一个实时的网络违规识别和响应系统。它位于被保护的内部网络和不安全的外部网络之间或位于内部网络的敏感部位。通过实时截获网络数据流，寻找网络违规模式和未授权的网络访问尝试。当发现网络违规或未授权访问时，基准入侵检测系统能够根据系统安全策略做出反应，包括实时报警，事件登录，自动阻断通信连接或执行用户自定义的策略程序等。基准入侵检测系统能够生成系统安全日志以利于系统安全审计并以开放数据库方式支持安全分析决策系统，从而为网络安全提供有效的保障。基准 IDS 具有以下显著特点：

- **基于分布式集中管理的工作模式**

  不同的分布式探针同时分布在不同的意欲保护的网络的网段或 VLAN，进行分布式监控，这些分布式探针通过一个可达的集中安全管理中心进行集中管理，达到入侵检测和集中安全管理的目的。IDS 这个设计思想能实现多网段安全的集中管理，也有助于实现大规模网络系统的入侵检测。

- **支持碎包重组（IP Fragment）**

  Baseline IDS 能对分散的 IP Fragment 数据包进行重组，可防止 teardrop 和 ssping 之类的碎片攻击。

- **支持安全策略的定制**

  Baseline IDS 提供了灵活易定制的安全策略管理机制，允许用户定义安全策略，确定系统应该关注那些行为和操作，并对这些行为进行响应。

- **支持行为规则的用户自定义**

  Baseline IDS 提供入侵行为和违规操作的定义模板，允许用户自定义规则库中没有的行为和操作，最大限度的检测入侵行为和违规操作。自定义规则弥补了规则库中入侵行为的局限性，大大地扩展了入侵行为的检测空间和范围，增加了检测的自由度。

- **支持安全域的自定义**

  Baseline IDS 能对安全域进行自定义，自行确定需要保护的网络范围，有效克服了入侵检测的盲目性，提高了入侵检测的效率和准确率。

  从某种程度上，能满足高带宽的通讯网络的需要，对与高带宽网络，我们可以布控多个探针在这一个网段，并给这些探针定义不同的安全域，每个探针负责一定范围的网络主机的入侵检测，解决了高带宽带来的处理能力有限的难题。

- **能精确判断入侵事件，误报和漏报率低**

  Baseline IDS 是基于入侵行为规则库和基于统计阀值而设计的，因而它对已知的攻击方式能准确的进行判断，误报和漏报率低。

- **黑盒子结构**

  Baseline IDS 的探测器设计成黑盒子结构，与网络的接口灵活，安装、使用方便易行。

- **支持与防火墙的互动使用(可选功能)**

  Baseline IDS 与防火墙配合使用，实现网络的双重保护。基准 IDS 将防火墙不能检测的入侵事件的有关信息转入防火墙的规则数据库中，以加强防火墙的防护功能。目前支持的防火墙类型为北京天融信防火墙和 NetScreen 防火墙。

- **支持系统的解码功能、对关键的访问进行记录和回放**

  Baseline IDS 在系统资源充足的情况下，可允许对关键的访问进行记录和再回放，便于管理员对新的攻击行为进行分析和处理。

- **不改变网络系统的拓扑结构及效率**

  Baseline IDS 不同于防火墙需要改变网络的拓扑结构，基准 IDS 类似于网络中的客户机，可并行的挂在需检测的网段上，不需要改变网络系统的拓扑结构，而且基准 IDS 不影响网络的运行效率，使用方便简洁。

- **系统安全可靠**

  Baseline IDS 采用了许可证制度，分布式探针和集中管理中心之间是实行保密通讯，保证了系统本身的安全性。

Baseline IDS 上述特点有机紧密的结合在一起，构成一个实时的、灵活的、实用的网络入侵预警情报及响应系统。

Baseline IDS 具备网络安全专家一样的入侵分析与判断能力，扩展了系统管理员的安全管理能力。Baseline IDS 为系统管理员提供了各种直观图形化工具和实时检测报警功能，极大地方便了系统管理员的安全管理。

3. Baseline IDS 体系结构

基准入侵检测系统是一个复杂的系统，系统的架构充分考虑到网络系统的规模、带宽流量、系统的工作效率及保证目标系统的可用性。基于这样的考虑，系统架构采用两个部分组成，即分布式探针和集中安全管理中心分别设计和布控，实现分布式检测和集中安全管理的大规模网络行为的安全检测、，最大限度地保证网络系统的安全性，帮助企业实现企业信息与网络系统统一的安全策略。

本章详细介绍 IDS 的体系结构，功能模块，工作原理。

- 体系结构
- 模块组成
- 工作方式
- 工作原理

3.1 Baseline IDS体系结构

基准 IDS 充分考察市场需求和系统管理与系统监控需要分开进行的需求，将系统分成两个部分：

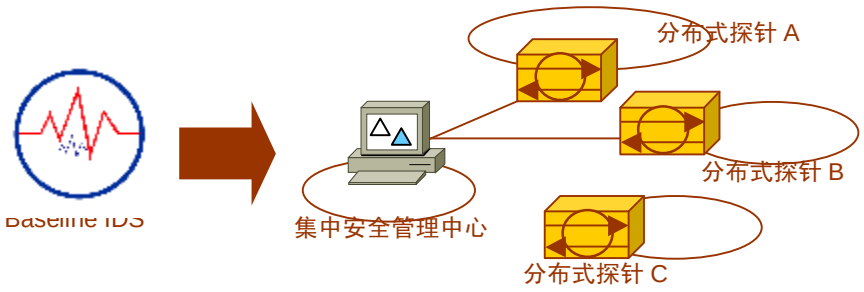
n 分布式探针 (IDS Sensor)

分布式探针（DS）为黑盒子结构，多个探针分别安装在不同的、独立的被保护的网段(Network Segment)上，每个探针全面监控进出被保护网段的数据流，根据安全策略的定义，通过实时截获与分析网络数据，利用独有的异常发现与模式发现的方法，结合人工智能技术寻找拒绝服务攻击行为（Denial of Services, DoS）、可疑行为（Suspicious Activity, SA）、攻击探测行为（Pro-Attack Probe, PAP）、未授权访问尝试(Unauthorized Access Attempt, UAA)和协议解码攻击（Protocol Decode, PD）等网络违规模式和行为，这些检测到的违规模式与攻击行为称为攻击事件（Event）。分布式探针将检测到的攻击事件实时报告集中安全管理中心，并根据安全策略的定义对这些攻击事件进行响应。

n 集中安全管理中心（IDS Console）

由于网络数据流的固有特性，IDS 分布式探针只能监测其所在网段上的数据流，因而在一个多网段的网络环境中需要多个分布式探针。为了适应这一需要，系统设计为集中管理的分布式结构。分布式探针根据安全策略将这些攻击事件及其详细信息传送给集中的统一的安全管理中心(IDS Console)，由 IDS Console 统一的管理，IDS Console 能够管理多个分布式探针的攻击事件。

当系统发现网络违规模式和行为时，系统根据安全策略作出响应，包括实时报警（Alert），事件登录（LogDB），自动阻断通信连接（RstSession），给安全管理员发送邮件（E-mail），给安全管理员发送传呼信息（Pager）和给网络管理系统发送 SNMP Trap 信息（SNMPTrap）等。如图 3 所示：



图表 3 入侵检测系统的构成

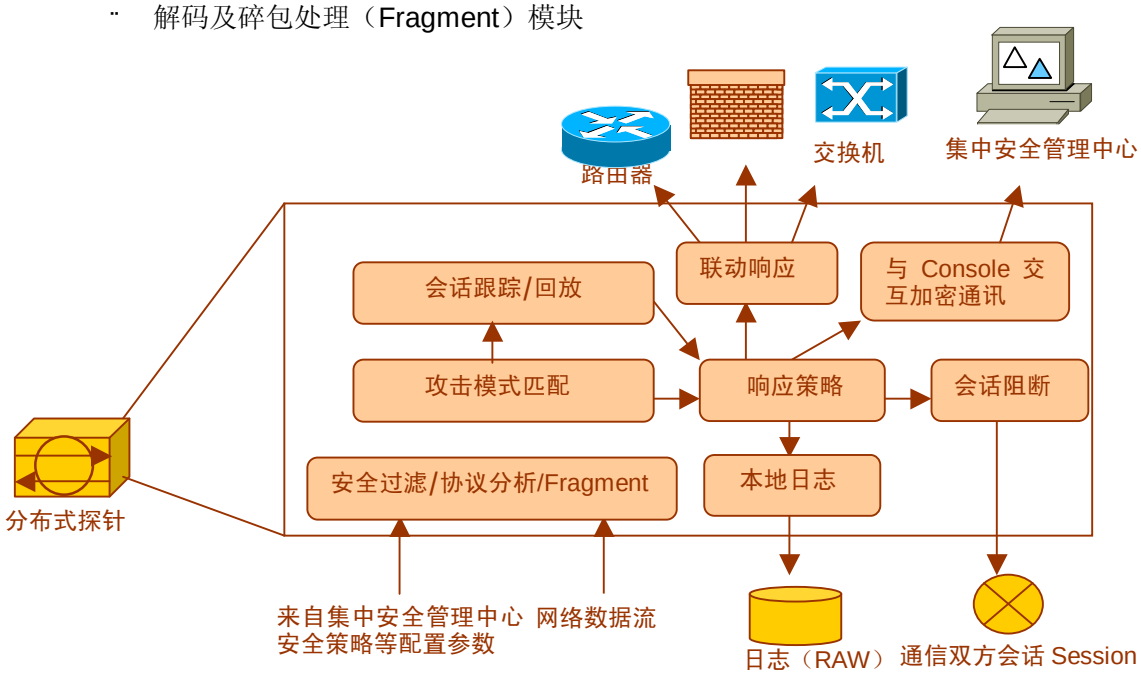
系统能够对指定时间段内的网络安全状况、安全事件情况进行审计、分析与综合，形成不同规格要求的分析报告，并能对网络安全状况提出早期的预警情报。

集中安全管理中心负责控制分布式探针，生成安全规则，接收报警和日志信息，提供网络安全审计报告，是直接面对用户操作的部分。

3.2 Baseline IDS模块结构

n 分布式探针模块组成

- 系统总控模块
- TCP/IP 数据包捕获模块
- 基于安全域包过滤模块
- 解码及碎包处理（Fragment）模块



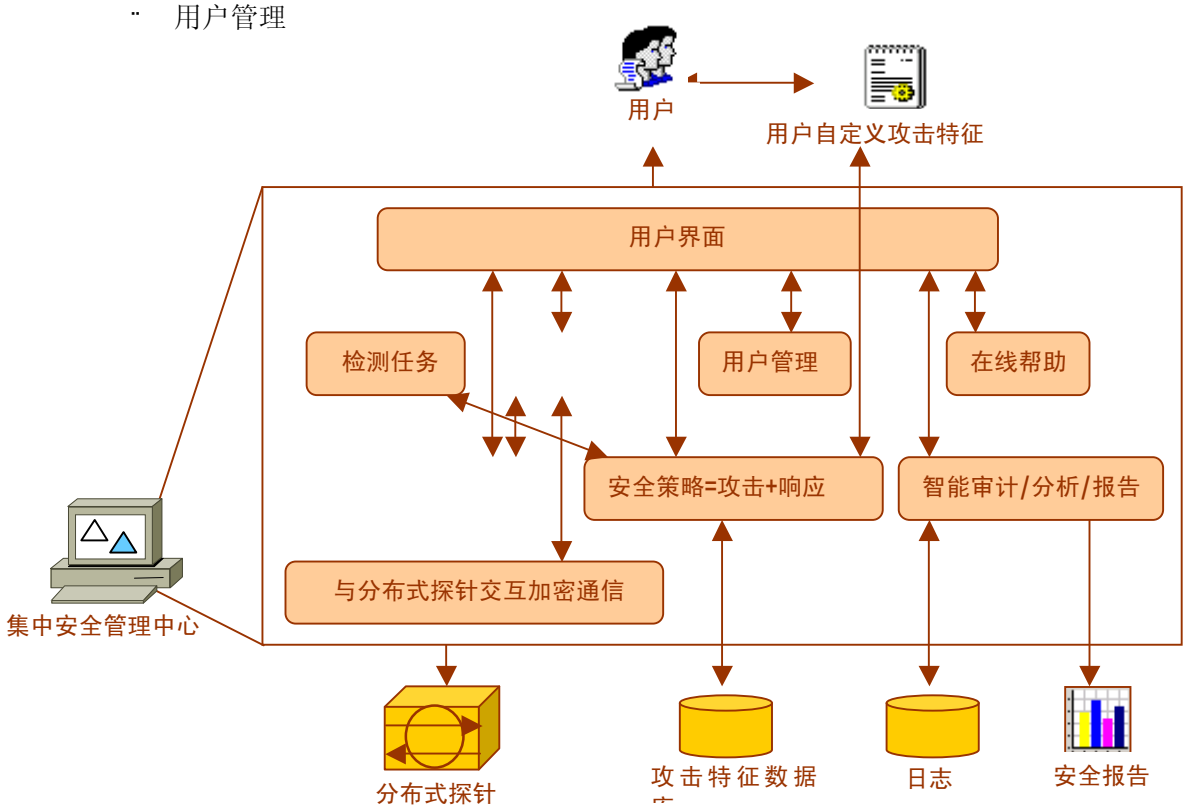
图表 4 分布式探针的模块构成

- 会话跟踪模块
- 协议分析模块

- 攻击模式匹配与用户规则匹配模块
- 规则库维护模块
- 策略响应模块
- 通信加密认证模块

n 集中安全管理中心模块组成

- 检测任务管理
- 安全中心管理
- 分布式探针管理
- 安全策略管理（包括自定义规则管理）
- 用户管理



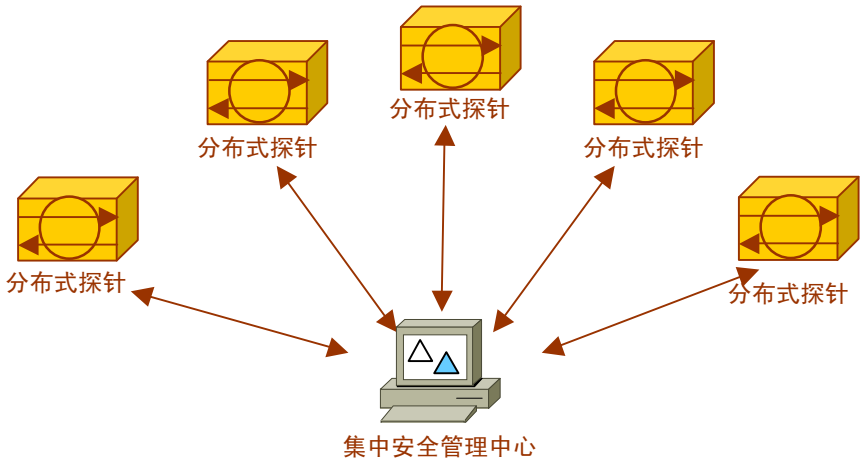
图表 5 集中安全管理中心的模块构成

- 日志审计分析报告管理
- 通信加密认证管理

3.3 Baseline IDS工作方式

Baseline IDS 采用集中管理的分布式网络安全监测工作模式。集中安全管理中心完成整个分布式安全监测预警系统的管理与配置。控测器监测它所在网段上的数据流，进行实时自动攻击识别和响应。

分布式探针安装在开放的外部网络与被保护的内部网络之间或内部网络中的敏感主机的网段上，对流经的数据进行实时检测。当一个企业内部的网络有多个出口或多个敏感部位的时候，可以在每一个需要监测的位置安放一个分布式探针。当分布式探针发现安全违规事件的时候，将有关的报警信息和日志信息发送到集中安全管理中心。这就是系统的分布式原则。如图 6 所示：

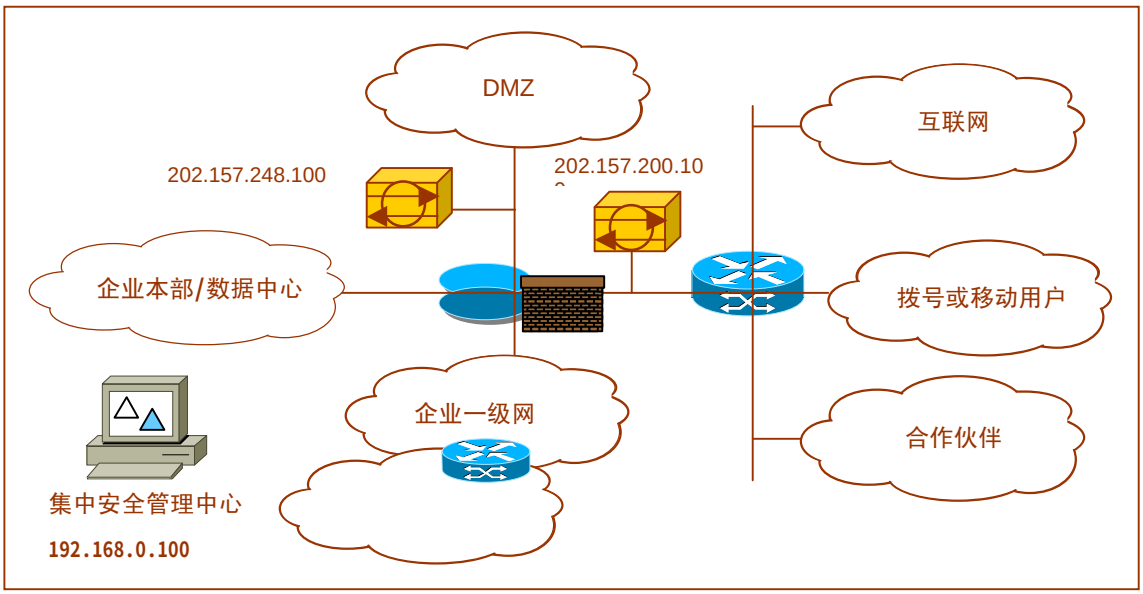


图表 6 分布式检测-集中式安全管理方式

企业的信息与网络系统的安全应该是可管理的安全，是集中统一的安全。分布式探针的设置虽然是分布式的，但是对于它的管理和控制却应该是集中的。集中安全管理中心是整个企业网络的集中安全管理中心，它负责启动分布式探针，向分布式探针加载安全规则、处理各个分布式探针发送来的实时报警和日志信息，定义和生成各个分布式探针应该执行的安全规则，提供对报警和日志信息的查询接口和生成系统安全审计报告等项任务。这就是系统的集中管理原则。

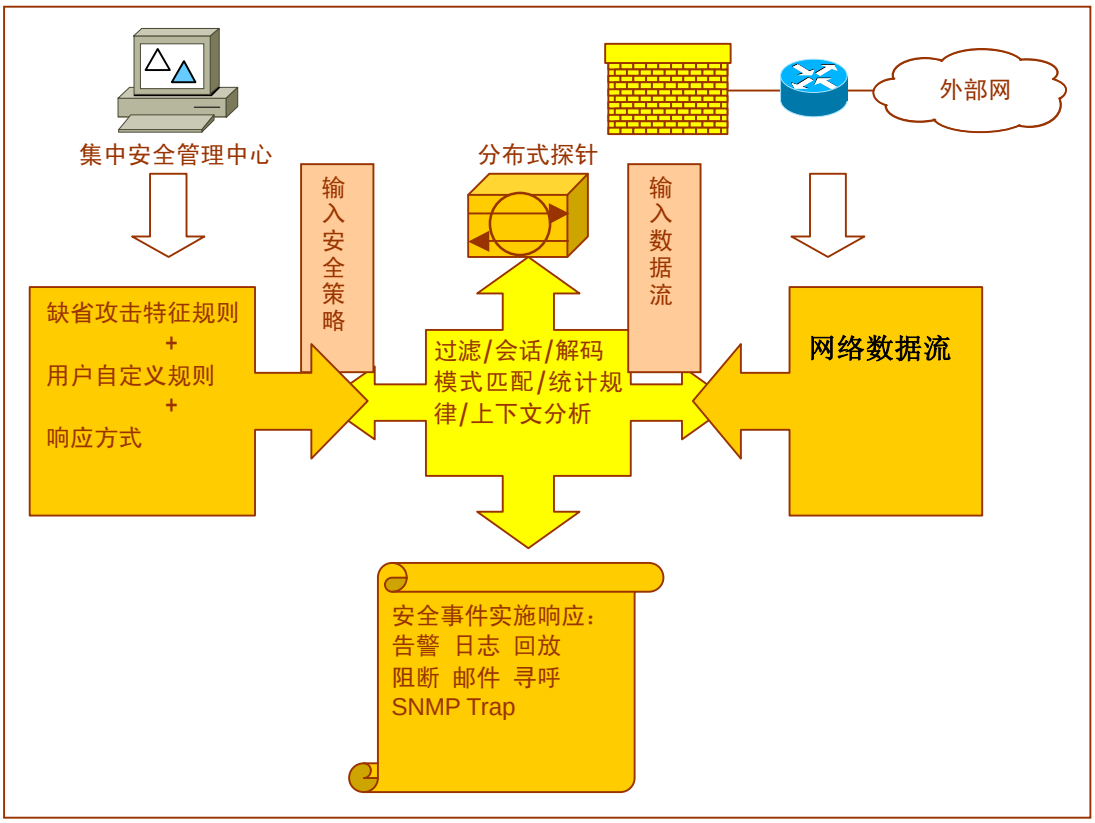
3.4 Baseline IDS工作原理

Baseline IDS 是一种网络实时自动攻击识别和响应系统。它运行于有敏感数据需要保护内部网络和不安全的外部网络之间，通过实时截取网络上的数据流，分析网络通讯会话轨迹，寻找网络攻击模式和其他网络违规活动。如图 7 所示；



图表 7 入侵检测系统布控示例

IDS 内置网络攻击特征数据库，在它所监测的网段上，它实时地分析网络数据流，识别违反用户定义的安全规则或匹配已知网络攻击模式的网络通信。识别的模式分为基于数据包上下文(Context)的监测和基于数据包内容(Content)的监测。基于数据包上下文的监测模式主要针对滥用网络服务协议或前后关联的网络操作序列，如执行了某些被认为是非法的命令或一些可疑的通信包的组合，如 IP Fragment 等；基于数据包内容的监测模式主要针对应用级攻击检查和违反系统安全规则的网络活动。如图 8 所示：



图表 8 入侵检测系统工作原理

当发现网络攻击或未授权访问时，入侵监测系统能够根据系统安全策略做出反应。寻找到网络攻击模式和其他网络违规活动时，IDS 可以进行如下响应方式：

- 集中安全管理中心告警(Alert)
- 记录网络攻击事件(LogDB)
- 实时阻断网络连接(RstSession)
- 关键部分回放(Replay)
- 邮件通知 (E-Mail)
- 扫描器策略联动(Scan)
- 通知网管中心(SNMP Trap)

IDS 采用透明工作方式，它静静地监视本网段数据流，对网络通讯不附加任何时延。

IDS 可以过滤和监视 TCP/IP 协议。系统管理员通过配置 IDS，可以按协议（TCP，UDP，ICMP），源端口，目的端口，源 IP/目的 IP 地址过滤。IDS 可以监测多种网络服务：包括电子邮件，文件传输，远程登录等等，并且所支持的服务随着 IDS 的发展不断地扩展。
IDS 还支持用户自定义的网络安全事件监视。

IDS 能够生成系统安全日志以利于系统安全审计并以开放数据库方式支持安全分析决策系统，从而为网络安全提供有效的保障。

4. Baseline IDS 性能指标

本章简要介绍 IDS 5.0 的综合性能、模块指标与技术参数。

- 综合性能
- 集中安全管理中心技术指标
- 分布式探针技术参数

4.1 Baseline IDS 5.0综合性能

类别	项目指标	内容概述
版本信息	生产厂家	北京杰马创新科技有限责任公司
	产品名称	基准入侵检测系统
	英文名称	**Baseline IDS**
	版本号，版本时间	**Version 5.0　2004/8/27**
系统功能	入侵行为检测功能（行为）	
	能够检测已知主要攻击的数量	**1312**
	攻击检测	支持
	违规操作检测	支持
	支持入侵检测方法	模式匹配，统计阀值分析、会话跟踪分析、**AI** 分析
	未知攻击行为的应对方法	目前系统版本没有学习攻击能力，不能自动识别未知攻击； 依靠用户自定义入侵行为规则来应对未知攻击。
	安全规则与策略管理功能（规则）	
	安全策略选择/定制	支持，允许用户选择或定制不同的攻击集合进行检测
	安全域定义	支持，支持不同范围的入侵检测
	用户自定义攻击规则	支持，提供 **GUI** 界面，允许用户对未知的或系统攻击行为数据库中没有的攻击行为或操作进行定义，以便系统能够检测这种行为或操作。
	响应方式的自由确定	支持，系统允许用户根据行为或操作的风险情况，自行选择响应方式。
	响应功能（响应）	
	告警能力	支持，集中安全管理中心根据事件的风险级别发出不同的声音告警。
	日志能力	支持，根据安全策略的要求，支持简单日志和详细日志记录能力。
	回放能力	支持，根据安全策略的要求，支持记录回放数据和回放。
	阻断能力	支持，根据安全策略的要求，对会话实施阻断，终止会话。
	Email 能力	支持，根据安全策略的要求，给安全管理员的邮箱发送告警邮件信息。
	Pager 能力	支持，根据安全策略的要求，给安全管理员的呼机发送告警邮件信息。
	SNMP Trap 能力	支持，根据安全策略的要求，给网管中心的邮箱发送告警信息。
	日志审计分析报告能力（审计）	
	事件审计	支持，支持不同粒度的事件分析与审计
	安全趋势分析	支持
	安全状况报告	支持，允许定制不同角色的报告
系统性能	数据获取能力/引擎速度	**100Mb** 之 **60%**流量测试，系统正常工作（无丢包现象）
	包重组（**Fragment**）	支持,支持 **8/16/32/64** 字节的碎包处理能力
	解码能力	支持
	安全策略的定义	支持
	用户自定义规则	支持
	分布式设计方案	支持 **50Sensors**
系统可用性	界面可用性	**GUI/Console,**黑盒子**/Sensor**
	支持的操作系统与应用	**Windows NT/2000 Console**
	产品的完善性	成熟的产品
	产品的安全性	安全可靠

集中安全管理中心（IDS Console）

指标体系	指标值
总体	
产品名称/型号	Baseline IDS Console V5.0，集中安全管理中心
产品类型	纯软件，用于管理基准 IDS Sensor V5.0 分布式设备，构成功能强大的入侵检测系统
产品介质	CDROM
工作限制	授权许可证（IP 地址、工作时间段）
运行平台	MS Windows 2000 Professional MS Windows NT 4.0 Workstation
主要性能参数	
安全策略管理	支持
用户自定义规则	支持，GUI 界面
参数配置	Console 参数，Sensor 参数
多用户分权管理	支持，超级用户，安全管理员，安全审计员
集中管理的探针数目	50
支持响应方式	告警，日志，阻断，回放，Mail，Scan，SNMP Trap
Console 与 Sensor 的通信	加密通信，高强度算法
日志审计	支持
日志综合分析	支持
日志趋势分析	支持
分析报告	支持
日志导出	支持

表格 1 集中安全管理中心性能指标

分布式探针（IDS Sensor）

分布式探针是入侵检测系统的数据采集、入侵检测分析、实施响应的核心设备，是入侵检测系统 IDS 的关键设备，为了保证处理效率，提高检测的准确率，特采取硬件结构。

- **探针系统平台（操作系统）**
  - 专用安全操作系统

- **探针系统工作效率**

  网络数据流截获引擎速度快，在 100M 网络中当网络流量保持在 60%时仍然可以监控 100%的包，每秒可以分析 17,000 个数据包。

- **主要性能**
  - 采用透明工作方式。接入系统，无需对网络的结构及设置作任何改动；对网络通讯不附加任何延时，不影响网络传输的效率。
  - 包重组能力强
  - 过滤器效率高
  - 解码能力强
  - 采用远程监控模式。可以对每个探测器进行远程配置，并支持加密通讯和认证。
  - 能进行运行状态实时监测，远程启停管理。
  - 具有多协议分析支持，可以进行应用解码，可进一步对数据包的内容进行分析处理。

- **主要型号**

  分布式探针 IDS Sensor 分为三个型号：
  - 工作组级分布式探针 Gminnova-IDS-Sensor-W1000（单 CPU，2*100MB）
  - 部门级分布式探针 Gminnova-IDS-Sensor-D2000（单 CPU，1*100MB+1*1000MB）
  - 企业级分布式探针 Gminnova-IDS-Sensor-E3000（双 CPU，2*1000MB）

- **主要配置**

  Sensor 出厂时，有如下缺省配置：
  - **管理口网络地址配置置文件**
    - 缺省 IP Address: 192.168.0.1
    - 缺省 IP Mask 255.255.255.0
    - 缺省 Port 7788,7789,7790
  - **授权许可证文件(以密文形式存放)**
    - 文件固定名称：IDS Sensor.key
    - 缺省 IP 范围为：0.0.0.0-255.255.255.255
    - 缺省时间范围为：三个月

- 用户文件
- 文件固定名称：IDSUser.Passwd
- 缺省内容：用户：admin　口令：admin(以密文形式存放)

- **安全域文件(以密文形式存放)**
  - 文件固定名称：IDSSensor.sa
  - 内容缺省为 0.0.0.0-255.255.255.255

- **策略文件(以密文形式存放)**
  - 文件固定名称：IDSSensor.policy
  - 内容缺省为空

- **工作日志文件**
  - 固定文件名称：IDS SensorWork.log
  - 记录内容：开机时间，关机时间；连接时间，断开时间，连接帐号；启动时间，停止时间；传输 Key 记录；传输策略记录；传输安全域记录。
  - 缺省时不记录日志文件。

- **事件日志文件**
  - 固定文件名称：IDS SensorEvent.log
  - 出厂时，设置为不记录此日志

- **控制参数文件**
  - 文件名：IDS Sensor.Option
  - 缺省未设置（不记录）

- **硬件配置**
  - **接口数量**
    - 两个 10/100Base-TX 接口 或者是 一个
    - 一个是数据监测（DATA）口；一个是通讯管理口(MANAGE)

根据用户需要配置，一个网络接口还是两个网络接口。如果是一个网络接口的话，数据监测口与通讯管理口合二为一。

  - **接口规范**
    - 网络接口：10/100BaseTX

- **电气性能**

- **电源**
  - 220V/50HZ，3.0A（最大），260W（最大）
- **环境规范**
  - 运行温度：0-45 摄氏度
  - 非运行温度：-20-65 摄氏度
  - 相对温度：10-90%@40 摄氏度，非冷凝

n 参考的安全规范及标准

- UL 1950
- EN 41003
- AS/NZS 3260
- AS/NZS3548 Class A
- CSA Class A
- FCC Class A
- EN 60555-2
- VCCI （ClassII）
- 抗干扰性
- IEC-1000-4-2（ESD）
- IEC-1000-4-3（辐射敏感性）
- IEC-1000-4-4（电快速瞬变）
- IEC-1000-4-5（电涌）
- IEC-1000-3-2（谐波）

5. Baseline IDS 运行环境

本章介绍了 IDS 系统的物理介质，运行该系统所要具备的硬件资源、网络资源以及操作平台。

- 装箱设备与物理介质
- 集中安全管理中心工作环境要求
- 分布式探针工作环境要求

5.1 Baseline IDS的物理介质

Baseline IDS 的介质主要以两部分组成，分布式探针部分安装在工控机系统中，以黑盒子的形式与网络相连；集中安全管理中心的以光盘形式发布。

介质	内　容
硬件 黑盒子	分布式探针 IDS Sensor 分布式探针系统超级用户的口令密码纸《超级用户口令》
网线	级联网线一根。
光盘	基准入侵检测系统的集中安全管理中心企业版软件的安装程序和系统文档的载体。
软盘	用户从销售商那里取得的授权许可证文件 IDS.key 或演示许可证文件 IDSdemo.key。
资料	与软件光盘和授权许可证配套的使用说明和参考资料： - 《基准入侵检测系统介绍》 - 《基准入侵检测系统系统安装手册》 - 《基准入侵检测系统用户使用手册》
包装	上述内容的包装盒。

表格 2 IDS 的物理介质

5.2 Baseline IDS运行环境

入侵检测系统的分布式探针与安全管理中心分别运行于两个独立的平台。

- **n** 集中安全管理中心 IDS Console
- **n** 分布式探针 IDS Sensor

5.3 集中安全管理中心的运行环境

集中安全管理中心的运行环境为 PC 机和服务器，它支持两种常用的操作系统的工作平台：Microsoft Windows NT Workstation 和 Microsoft Windows 2000 Professional。 具体要求如下。

Windows NT Workstation 系统需求

项目	最小系统需求
处理器	200MHz Pentium Pro（推荐 300MHz Pentium）
操作系统	安装了 Service Pack 6 的 Windows NT Workstation 建议使用独立、专用计算机系统安装使用本系统。
其他软件	Microsoft IE 4.X 或更高版本用于运行 HTML 帮助 Microsoft Word 97/2000 或更高版本用于查看 RTF 报告 Adobe Acrobat Reader 4.x 或更高版本用于查看 PDF 报告
内存	通常侦测：80MB 大规模侦测：128MB（推荐 256MB）
硬盘	从文件安装需要 180MB，从 CD 安装需要 60MB。 运行时：55MB + 2.5MB 每 100 个主机 强烈建议 NTFS 分区
用户权限	本地或域管理员
网络	连接到一个活动网络中的 Ethernet 或 Token Ring
协议	TCP/IP
MDAC	2.1 或更高版本
显示	支持最少 256 色、800x600 分辨率的显示器。建议使用 1024x768，24bits 彩色显示环境。

表格 3 系统需求 Windows NT 4.0 Workstation

注意：IDS V5.0 不支持 Windows NT 3.51, Windows NT Server, Windows 2000 Server, 或 Windows 2000 Advanced Server。可能在这些环境中能够运行，但不保证系统的稳定性和可靠性。

Windows 2000 Professional 系统需求

项目	最小系统需求
处理器	200MHzPentium Pro（推荐 300MHz Pentium）
操作系统	Windows 2000 Professional 建议使用独立、专用的计算机系统安装使用本系统。
其他软件	Microsoft IE 4.X 或更高版本用于运行 HTML 帮助 Microsoft Word 97/2000 或更高版本用于查看 RTF 报告 Adobe Acrobat Reader 4.x 或更高版本用于查看 PDF 报告
内存	通常侦测：80MB 大规模侦测：128MB（推荐 256MB）
硬盘	从文件安装需要 180MB，从 CD 安装需要 60MB。 运行时：55MB + 2.5MB 每 100 个主机 建议 NTFS 分区
用户权限	本地或域管理员
网络	连接到一个活动网络中的 Ethernet 或 Token Ring
协议	TCP/IP
MDAC	2.5
显示	支持最少 256 色、800x600 分辨率的显示器。建议使用 1024x768，24bits 彩色显示环境。

表格 4 系统需求 Windows 2000 Professional

5.4 分布式探针的运行环境

分布式探针为黑盒子（专用工业控制机）结构，对外的连接界面为一个接口 或者是两个接口。
系统出厂时，管理口缺省的 IP 地址为：192.168.0.1，地址掩码为：255.255.255.0，因此，要使系统开展工作，需要给分布式探针分配并设置一个 IP 地址和地址掩码。同时，这一地址必须是受保护网段内的地址与掩码。

由于分布式探针的文件都是加密保护的，探针的配置需要集中安全管理中心进行配置。不能通过在分布式探针上，安装显示器、键盘和鼠标来直接配置。这样的配置，系统不能正常工作。
分布式探针内部运行平台是专用安全操作系统。

注意： 分布式探针的运行环境关键在于统一的规划、布控和安装。分布式探针的参数配置尤为重要。关于分布式探针的配置请参阅其他章节，它关系到能否正常使用整个系统的关键。

6. 功能介绍

基准入侵检测系统作为一个网络安全防御系统，它本身也必须具有较强的安全级别。这就要求入侵检测系统不仅具有系统登录身份验证，系统锁定，系统解锁等安全控制能力，而且还具有对使用本系统的用户进行严格管理的能力。本系统中，我们将所有的用户分为三大类：系统管理员，安全管理员，安全审计员。系统管理员具有本系统的所有权限，安全管理员相对于系统管理员来说，缺少了用户管理的权利，其它的功能完全一样。而安全审计员所拥有的权利最少，他只能对已检测到的网络攻击事件进行审计，而不具备其它的权利。

下面我们将开始介绍系统的使用方法。

6.1 系统登录

步骤 1 将鼠标移动到入侵检测系统快捷方式图标上，然后在本图标上双击鼠标左键；如图 **9** 所示：

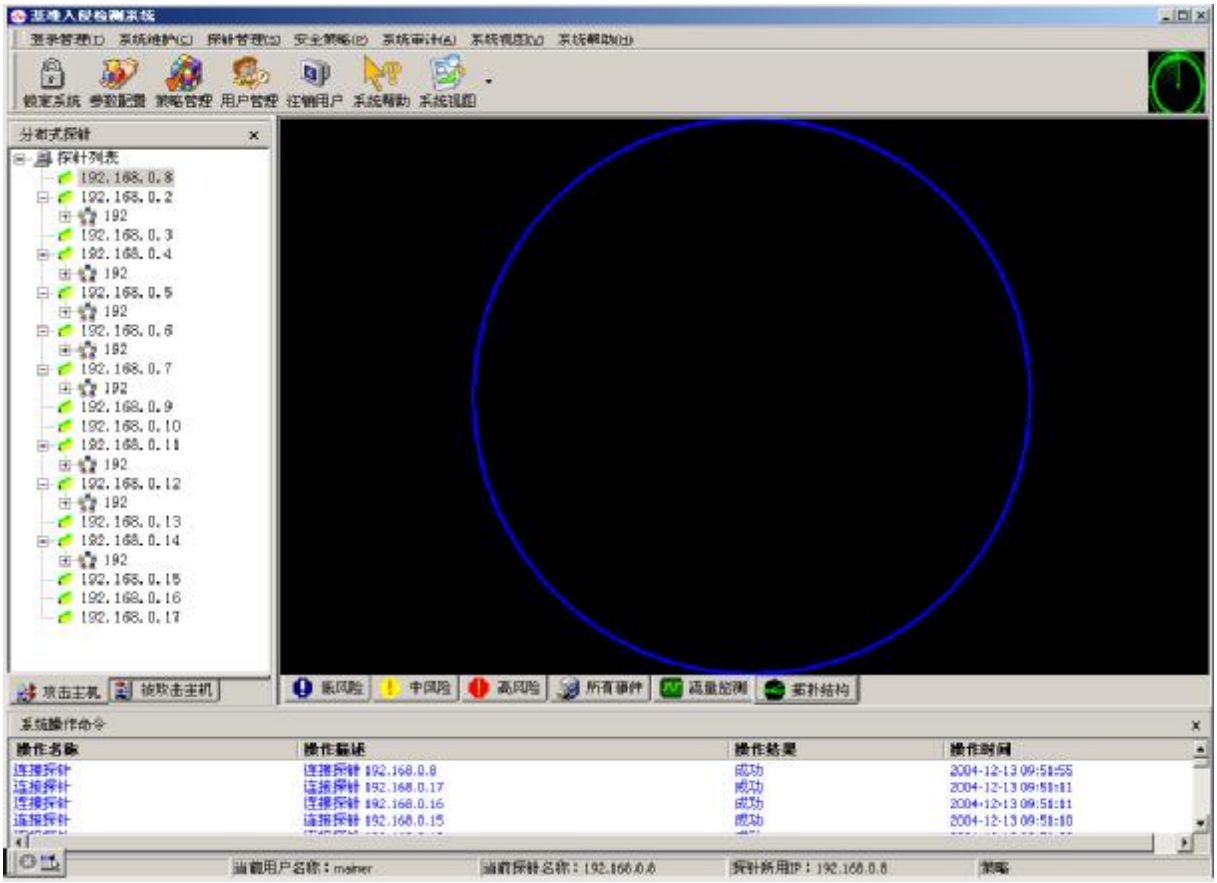
图表 9 入侵检测系统快捷方式图标

步骤 2 此时系统将弹出一个用户登录界面，请填写用户名和密码，然后点击“登录”按钮，系统将对用户进行身份验证；如图 **10** 所示：

图表 10 登录系统身份验证

骤 3

n 如果身份验证成功，系统将开始进行各种初始化工作，最后显示所示的界面，这表示系统已经完成登录，处于运行状态；如图 **11** 所示：



图表 11 入侵检测系统界面

n 如果身份验证没有成功，系统将取消本次身份验证操作，并且开始下一次的验证。本系统允许用户连续进行三次身份验证，如果三次都不成功，系统将自动停止身份验证。

6.2 锁定系统与系统解锁

当用户执行完锁定系统功能后，系统仍处于运行状态，可以接收探针发送过来的告警事件、对这些告警事件进行各种处理，以及其它的各种运行态功能。但此时系统的运行界面将不再是图 **11** 所示，而是缩小为如图 **13** 所示的操作系统状态栏的一个小的图标。在此状态下，用户是无法查看各种告警信息的。通过执行系统解锁功能，可以使系统恢复到如图 **11** 所示的状态。

6.2.1 锁定系统

步骤 1 将鼠标移动到 “登录管理” 菜单上，然后单击“锁定系统”子菜单；如图 **12** 所示：

图表 12 锁定系统子菜单

步骤 2 此时，系统将最小化为 **Windows** 操作系统右下角任务栏窗口中的一个小图标；如图 **13** 所示：

图表 13 系统处于锁定状态时的显示形式

6.2.2 系统解锁

步骤 1 将鼠标移至操作系统右下角任务栏中，右键单击本系统图标，此时，将出现一个弹出式菜单，单击本菜单中的“系统解锁”子菜单，或者直接在任务栏中双击系统锁定状态图标；如图 **14** 所示：

图表 14 系统解锁菜单

步骤 2 在用户重新登录系统界面中填写用户名称和用户密码进行身份验证；如图 **15** 所示：

图表 15 用户重新登录系统身份验证界面

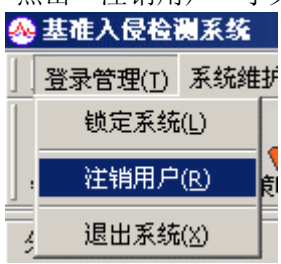
说明：

只有锁定本系统的用户才可以解锁本系统，在用户重新登录系统身份验证窗体中，系统自动在用户名称一栏中显示锁定本系统的用户名称，并且本用户名称不允许修改，用户只需要在用户密码一栏中填入锁定本系统的用户密码，然后点击“确定”按钮，通过身份认证后即可解锁本系统。

6.3 注销用户

在本系统中， 不同的用户具有不同的权限，在不退出本系统的情况下，可以通过注销用户功能在不同的用户间进行切换。

步骤 1 将鼠标移动到“登录管理”菜单中，点击“注销用户”子菜单；如图 **16** 所示：

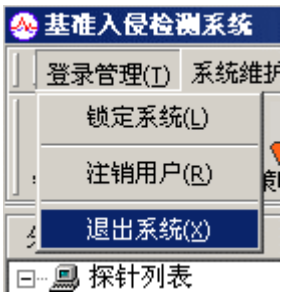


图表 16 注销用户子菜单

步骤 2 此时将重新弹出系统登录界面，填入用户名称和用户密码即可。

6.4 退出系统

步骤 1 将鼠标移动到 “登录管理” 菜单中，点击“退出系统”子菜单；如图 **17** 所示：



图表 17 退出系统子菜单

步骤 2 同重新登录系统，要求用户在退出系统前进行身份认证，如图 **7** 所示，通过身份认证后方可退出系统，否则系统弹出消息，取消此次操作。如图 **18** 所示：

图表 18 身份认证失败

7. 系统维护

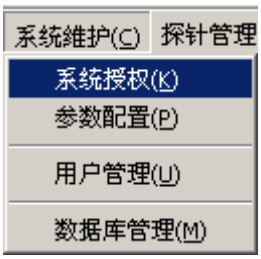
7.1 功能介绍

一个系统的正确运行，需要各种正确的配置参数，而且系统在长期的运行过程中，需要进行不断的维护，以保证系统能够高效、灵活、稳定的运行。在本系统中，所有的这些工作，都通过 “系统维护” 菜单的子菜单来实现。
下面将具体介绍各个子菜单的功能。

7.2 系统授权

用户购买基准入侵检测系统时，我们将会提供一张许可证软盘，本许可证软盘中包含有一个许可证文件 IDS.Key，在本许可证文件中包含了用户的各种信息以及产品信息，系统运行时需要读取这些信息。第一次运行本系统时，请执行系统授权操作。
请您保存好您的许可证软盘，一旦丢失，请立即与我们联系。

步骤 1 将鼠标移动到系统维护菜单，点击“系统授权”子菜单；如图 **19** 所示：

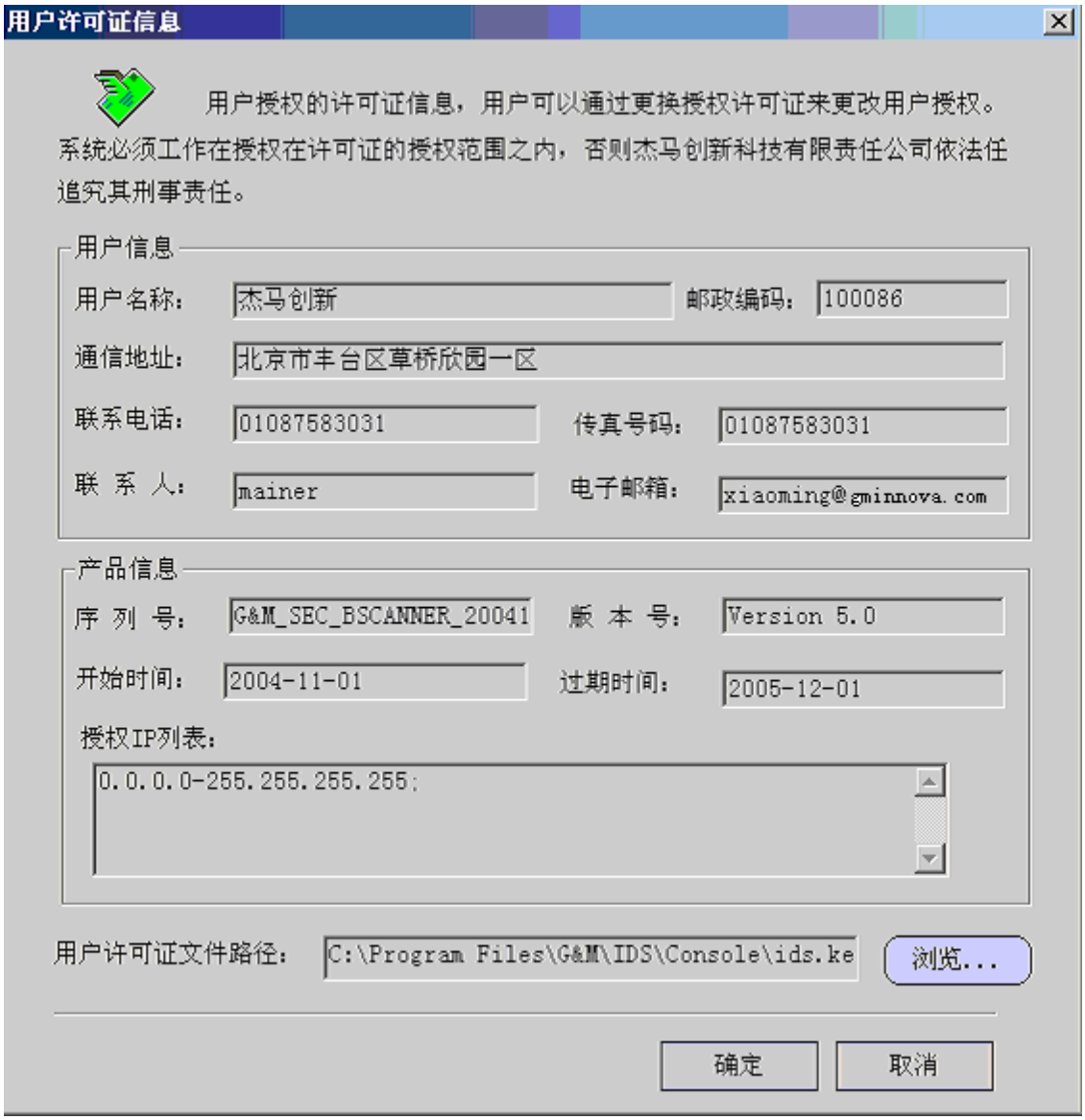


图表 19 系统授权子菜单

步骤 2 此时，系统将弹出“选择/更换/显示许可证” 界面，点击“浏览”按钮打开许可证文件选择窗口，

在该窗口中找到包含本系统许可证文件的目录，并选中许可证文件 IDS.Key，如图 20、图 21 所示：

图表 20 许可证选择



图表 21 许可证信息

说明：

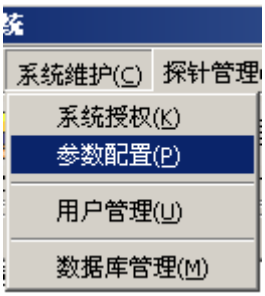
- 如果许可证没有过期，则系统将在图 **13** 中显示本许可证的一些信息，否则，将提示 “许可证版本错误” 信息。
- 因为系统在每次起动时都将读取本许可证文件，因此建议用户将许可证文件从软盘中拷贝到硬盘中，然后在运行系统授权时，选中硬盘中的本许可证文件。

7.3 配置参数

对于各种各样的，破坏程度不同的网络入侵事件，用户可以指定不同的响应方式，包括声音告警，给管理员发手机短消息，发电子邮件，发传呼等。关于如何为每一个网络入侵事件设置响应方式，请参考 “策略配置” 功能。 对于某一特定的网络入侵事件，当探针检测到本入侵事件时，报告安全管理中心，安全管理中心读取本次告警事件的响应参数，然后按照用户所设置的响应方式进行响应。不同的响应方式有不同的参数设置，请在下边的参数配置窗体中进行各种响应参数的设置。

7.3.1 进入工作参数配置窗体

将鼠标移动到系统维护菜单上，点击“参数配置”子菜单；如图 **22** 所示：



图表 22 配置参数子菜单

7.3.2 系统参数

系统参数设置包括告警脚本语言设置和告警声音文件设置。用户可以为一个网络告警事件指定一个告警脚本，安全管理中心接收到本网络入侵事件的告警时，就将执行本告警脚本。用户也可以为网络告警事件指定告警声音文件。选用声音告警时，请为高中低三种风险级别的告警事件指定不同的告警声音文件。

点击系统参数标签，进行系统参数配置；如图 **23** 所示：

图表 23 安全管理中心工作参数配置

7.3.3 SMS 告警

SMS 告警参数主要设置使用手机短消息这种响应方式时用到的各种参数，包括注册手机号码，接收人手机号码等。

点击 SMS 告警标签，进行 SMS 告警配置；如图 24 所示：

图表 24 SMS 告警参数设置

7.3.4 Scan 告警

Scan 告警设置与我们的另一产品 iSCAN 联动时使用的各种配置参数，包括 iSCAN 的 IP 地址，iSCAN 的联动端口号以及扫描对象等。点击 “扫描确认”，进行联动配置；如图 25 所示：

图表 25 扫描确认

7.3.5 Email 告警

Email 告警设置使用 Email 告警响应方式使用到的各种配置参数，包括邮件服务器地址，收件人地址等。点击 “Email 告警”，进行相关参数配置；如图 26 所示：

图表 26Email 告警参数设置

7.4 用户管理

分权管理机制是安全系统重要的安全管理办法预措施，系统将不同的操作划分为不同的权限，由不同权限的用户分别执行和操作。

入侵检测系统将用户分成三个不同的级别。用户管理还提供了用户口令修改、添加用户、删除用户、用户权限配置等功能。

7.4.1 用户的三级权限

- 超级用户

系统管理员可以进行用户管理、安全管理和安全审计的分析；

- 安全管理员

安全管理员能进行安全管理和审计分析；

- 安全审计员

安全审计员的权限最低，它只能对日志数据库进行审计分析。

7.4.2 进入用户管理

步骤 1 将鼠标移动到“系统维护”菜单上，点击“用户管理”子菜单；如图 **27** 所示：

图表 27 用户管理子菜单

步骤 2 此时，本系统将弹出一个用户管理界面，如图 **28** 所示：

图表 28 进入用户管理

7.4.3 用户管理的功能描述

利用用户管理，可以根据要求添加新用户；修改用户口令，增加系统的安全性；删除不必要的用户等等。

（1） 添加用户

在图 **28** 所示的用户管理界面中，用户可以单击“添加”按钮添加一个新用户，用户只需在弹出的对话框中的各个文本框中填写新用户的相关信息，单击“确定”便完成了添加新用户的操作，同时在图 **28** 中的列表框中会显示新用户的信息。如图 **29** 所示：

图表 29 添加用户

（2） 修改密码

如果用户长时间使用同一个密码，很有可能造成整个系统的不安全，因此，经常的更换密码是有必要的。在图 **28** 用户管理界面中选择要修改密码的用户，单击“更改密码”按钮，进入“更改密码”界面，确任旧密码后，输入新密码，单击“确定”；如图 **30** 所示：

图表 30 更改密码

（3） 删除用户

删除长期不使用的用户名和不必要的用户是必需的。在图 **28** 用户管理界面中选择要删除的用户，单击“删除”，出现下面对话框，单击“是”确认删除；如图 **31** 所示：

图表 31 删除用户确认

7.5 数据库管理

本系统使用的数据库是 **MS SQL Server** 数据库，数据库里有很多数据库表。其中最重要的是告警事件表和回放事件表，它们的数据量很大，有可能充满系统盘，而且这两个数据库表的信息非常重要，所以经常做备份是必需的。数据库管理实现这一功能。

数据库管理工具包括查看数据库表、备份数据库表、导入数据库表、清空数据库表等，

7.5.1 进入数据库管理界面

步骤 1 将鼠标移动到“系统维护”菜单上，点击“数据库管理”子菜单；如图 **32** 所示：

图表 32 数据库管理子菜单

步骤 2 此时，本系统将弹出一个数据库管理界面，如图 **33** 所示：

图表 33 数据库管理界面

7.5.2 数据库管理的功能描述

n 查看数据库表

查看数据库表功能，能够给用户：记录数是多少，应该什么时候开始备份等信息。在图 **25** 数据库管理界面点击“查看数据库表”就可以进入数据库表信息界面；单击“告警事件数据库”单选按钮可以查看告警事件数据库表的信息；单击“回放事件数据库”单选按钮可以查看回放事件数据库表的信息；如图 **34** 所示：

图表 34 查看数据库表

说明：

点击“确定”即可回到主窗体。

n 备份数据库表

备份数据库表提供了备份两个最重要的数据库表的功能，它能够将数据库内的数据备份到你想要的任意目录下的文本文件中，保证了重要的数据不丢失。备份完成后，该数据库表的记录将被清空。在图 **25** 数据库管理界面点击“备份数据库表”就可以进入备份数据库表界面，通过点击“浏览”按钮可以设置要备份数据库表的文件和目录。通过两个单选按钮，可以备份不同的数据表。单击“确定”，开始备份；如图 **35** 所示：

图表 35 备份数据库表

备份完成时系统给予提示；如图 **36** 所示：

图表 36 数据库备份完成

n 导入数据库表

导入数据库表提供了将已经备份了的数据，在需要的时候导回到数据库中的功能。导入数据库表是备份数据库表的逆过程。在图 **25** 数据库管理界面，点击“导入数据库表”进入导入数据库表界面，通过点击“浏览”按钮可以设置要导入数据库表的文件和目录。通过两个单选按钮，可以导入不同的数据表。单击“确定”开始导入数据；如图 **37** 所示：

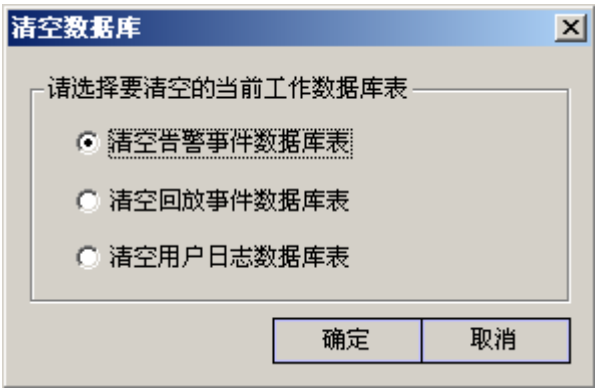
图表 37 导入数据库表

导入完成时系统给予提示；如图 **38** 所示：

图表 38 数据库表导入完成

n 清空数据库表

清空数据库表提供清除数据库表中的所有记录的功能。在图 **25** 数据库管理界面，点击“清空数据库表”可以进入清空数据库表界面，通过三个单选按钮，可以选择清空不同的数据库表，单击“确定”开始清空；如图 **39** 所示：

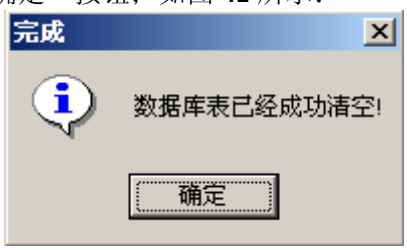


图表 39 清空数据库表

为了防止错误的操作造成不必要的损失，在确定清空之前会还有一次确认，能有效的防止误操作，在确认无误时，点击“是”，便清空了数据库表，选择“否”，将取消此次操作；如图 **40** 所示：

图表 40 数据库清空确认

选择“是”，清空完成后，单击“确定”按钮；如图 **41** 所示：



图表 41 数据库表清空完成

说明：

在图 **33** 界面中还有一个“退出”按钮，单击它将退出数据库管理界面。

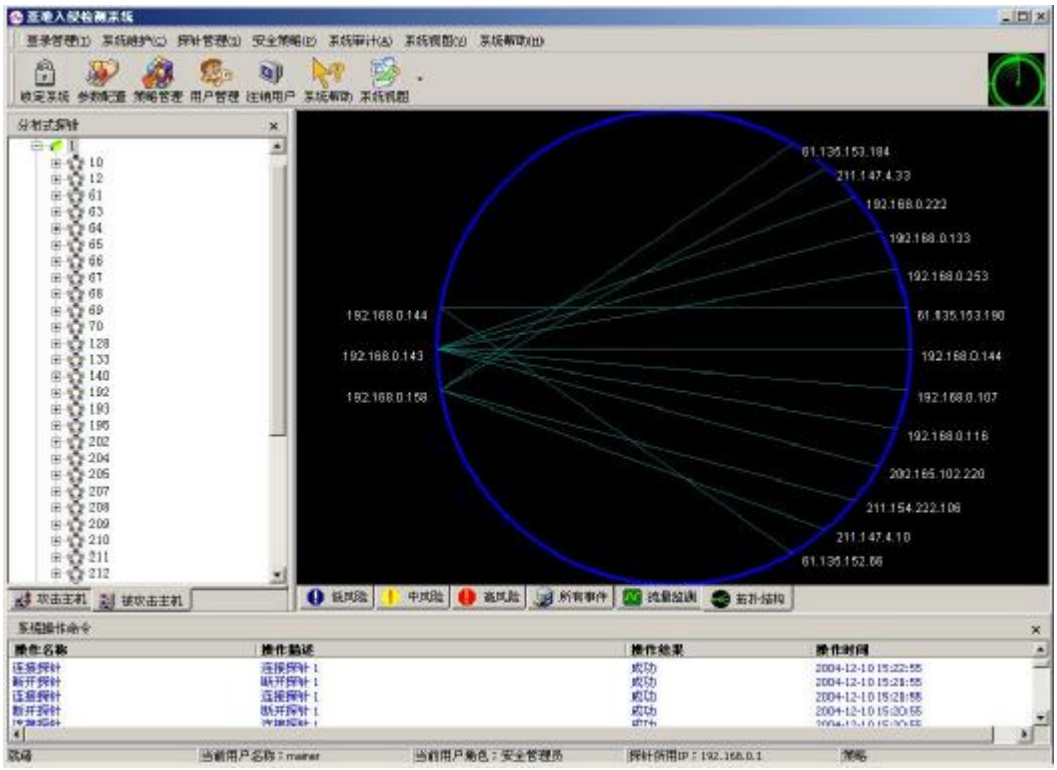
Baseline

8. 系统视图

8.1 功能介绍

我们已经在图 **3** 中看过系统的主界面，在这里，我们将要介绍如何对系统主界面进行设置，以使主界面看起来更美观，更舒服。

首先，我们对系统主界面作一个介绍。本系统的主界面由六大部分组成：主菜单，工具栏，探针列表视图，告警事件列表视图，系统操作命令列表视图，状态栏；如图 **42** 所示：

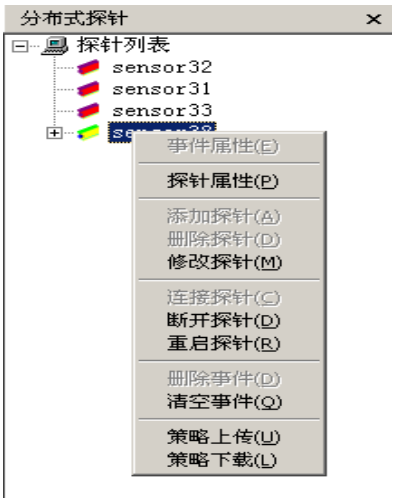


图表 42 界面划分图

8.1.1 各部分功能的描述

- 主菜单：包括各类子菜单，主菜单和它所包括的子菜单完成整个系统的所有功能。本系统共包括七个主菜单。
- 工具栏：工具栏的功能已经包含在子菜单中，工具栏的工具完成我们常用的几个功能。工具栏处于主菜单下边，由八个工具组成。
- 探针列表视图：本视图分为两部分：攻击者主机列表视图，被攻击者主机列表视图。两部分的显示内容基本一样，只是在显示告警事件时有所不同，在下面， 我们会具体介绍。

系统在每一个列表视图中显示所有的探针名称，选择一个探针，右击鼠标弹出菜单，对于弹出式菜单中各个子菜单的功能，我们将在后面具体介绍。如图 **43** 所示：

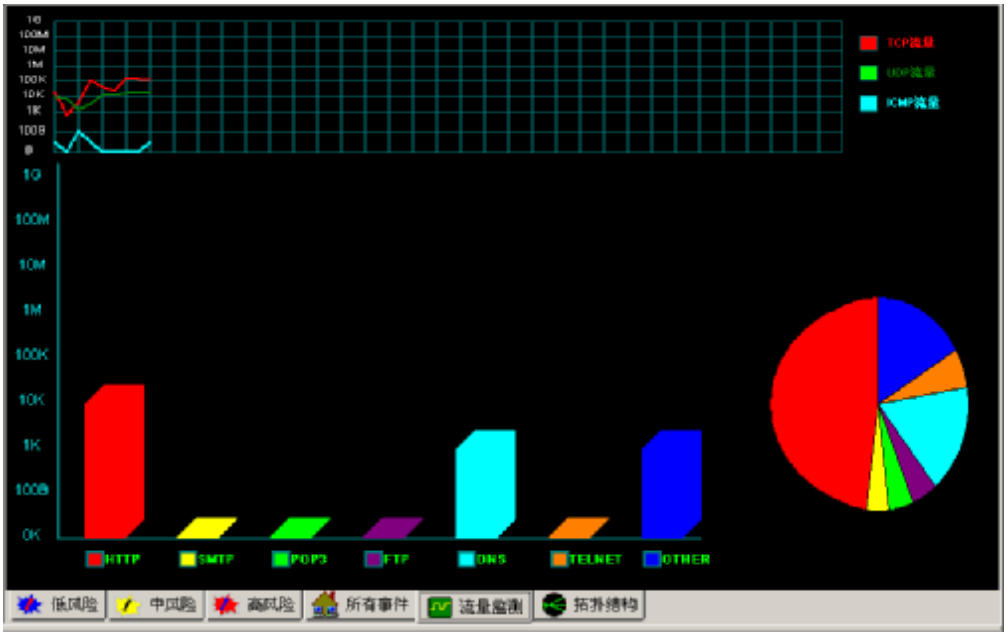


图表 43 列表视弹出式菜单

- 告警事件列表视图：本视图共有六部分构成：低风险，中风险，高风险，所有事件，流量监测，拓扑结构。
  - 在低风险视图中显示风险级别为低的网络入侵告警事件；如图 **44** 所示：

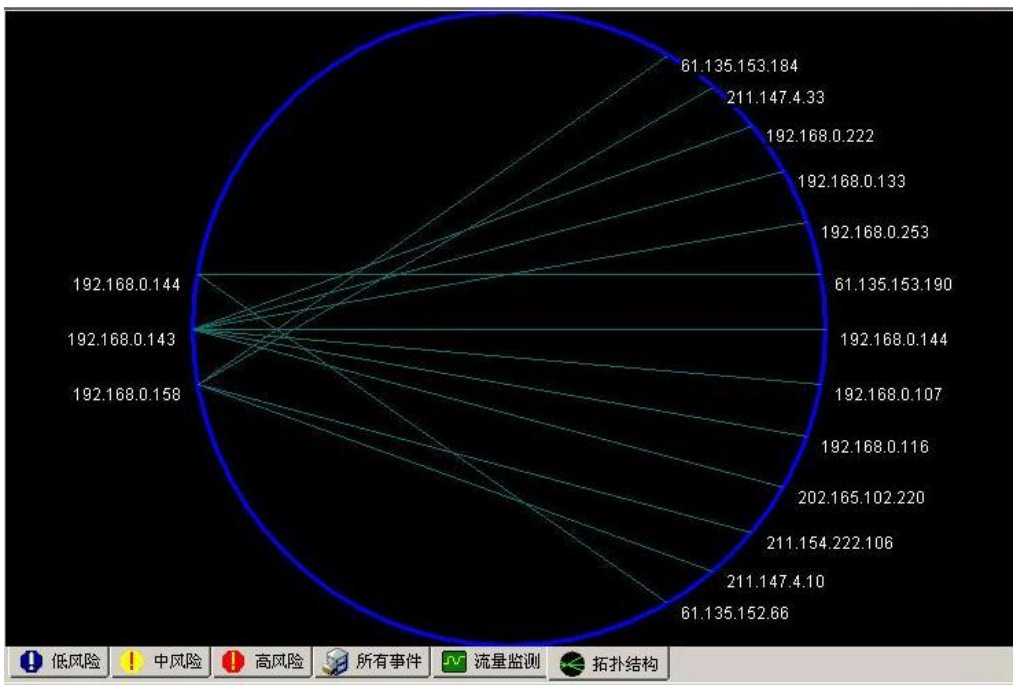
图表 44 低风险视图

- 中风险，高风险显示相应的级别的网络入侵告警事件。流量监测显示整个网络的数据流量，包括 **Tcp,Upd,Icmp**，以及 **Http,Smtp,Pop3,Ftp,Dns,Telnet,Other** 等，其中前者以坐标图形式显示 **5** 秒钟的流量，后者以柱状图和饼图的形式显示到目前为止的累加值。如图 **45** 所示：



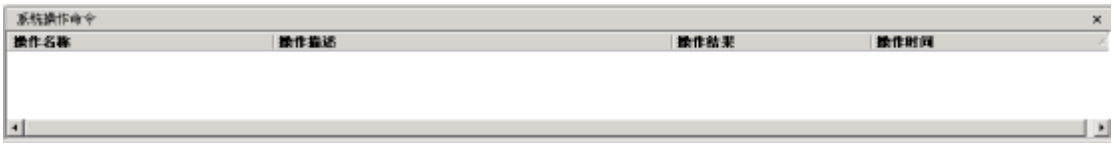
图表 45 流量监测视图

- 拓扑结构显示当前的一个网络连接（如图 **5-4**），每条连线表示一个网络连接，在连线的两边，系统将写出本次连接的源地址和目的地址。如图 **46** 所示：



图表 46 拓扑结构视图

- 系统操作命令列表视图：在本视图中，系统将显示到目前为止所有系统操作，包括探针的连接、断开，策略的更改等等。每一个操作包括操作名称，操作描述，操作结果，操作时间等四个属性；如图 **47** 所示：



图表 47 系统操作命令列表视图

- 状态栏：状态栏主要由四部分组成，系统运行状态，当前用户名称，当前探针名称，探针所用 **IP**；如图 **48** 所示：

图表 48 状态栏视图

8.2 显示、隐藏树列表

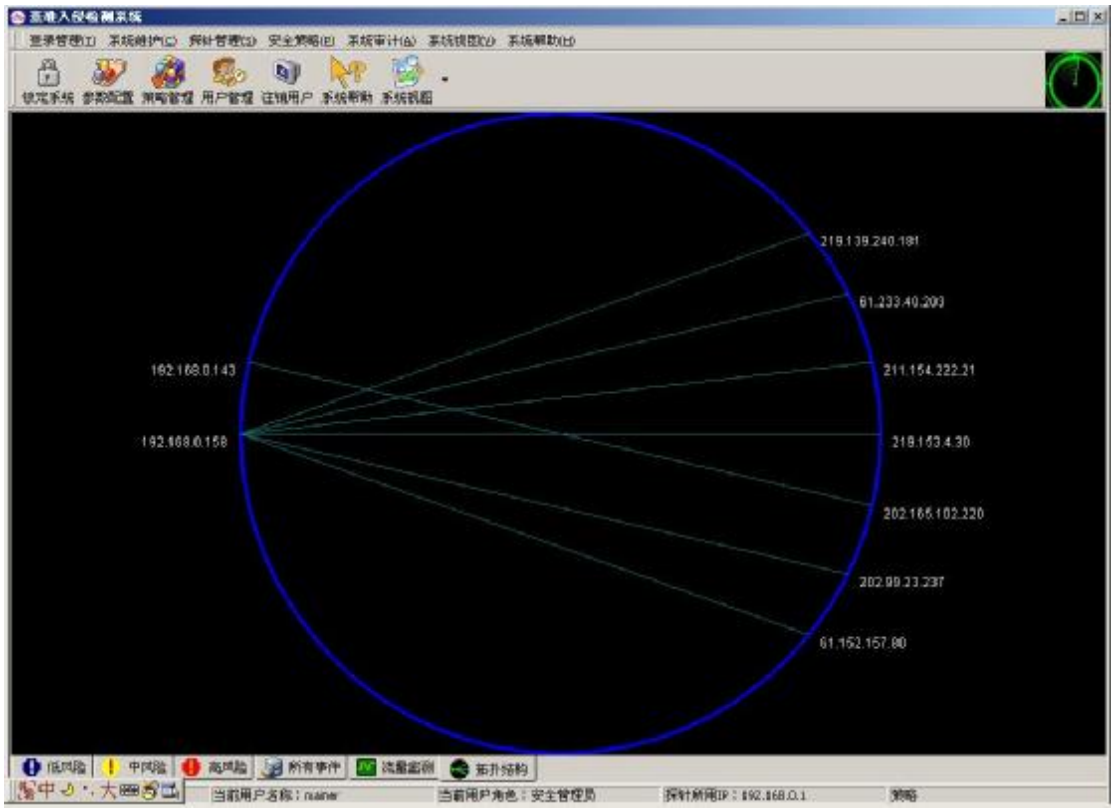
将鼠标移动到图 **41** 系统视图菜单上，点击树列表子菜单，系统将在树列表的显示、隐藏状态间进行切换。 表示显示状态，否则表示隐藏状态；如图 **49** 所示：

图表 49 树列表子菜单

或者点击状态栏中的系统视图按钮进行设置；如图 **50** 所示：

图表 50 工具栏树列表视图

隐藏树列表视图后的主界面；如图 **51** 所示：



图表 51 隐藏树列表视图后的系统显示状态

8.3 显示、隐藏信息栏

请参考显示、隐藏树列表。

9. 探针管理

9.1 功能介绍

探针管理功能模块使得用户可以对所有的探针进行各种各样的设置、操作，包括初始化、连接和断开探针等等。探针在入侵检测系统中起到一个后台检测功能，而入侵检测预警和响应系统安全管理控制台则起到一个前台的管理功能，本主菜单 “探针管理” 是探针和安全管理控制台进行交互的主要部分，它包含了对探针的大部分操作。

下面对 “探针管理” 主菜单中的各个子菜单逐一进行介绍。

9.2 添加探针

添加探针功能是整个入侵检测系统工作的前提和必要条件。添加探针对要参与工作的探针进行基本信息的设置，为正式工作做准备，它是探针开始工作的第一步，也是很关键的一步。通过添加探针功能，用户可以在安全管理控制台中添加一个新的探针。用户第一次购买到入侵检测系统时，探针的出厂 **IP** 地址为 **23.1.1.1**，本网络地址显然不是用户的内部网地址，用户可以自行修改。在执行本次操作时，请记住一点，新的探针不能同已有的探针重名，否则，系统将报错。添加探针的具体步骤如下：

步骤 1 将鼠标移动到探针管理菜单上，点击“添加探针”子菜单；如图 **52** 所示：

图表 52 添加探针子菜单

或者在左边的探针列表中点击鼠标右键，在弹出式菜单中点击添加探针子菜单。

步骤 2 此时，系统将开始添加探针的操作，本操步分为三小步：

1) 在下面出现的对话框中填写探针名称、探针地址和探针的简要描述等信息，填写完成后，单击“下一步”；如图 **53** 所示：

图表 53 添加探针第一步

2) 单击“下一步”；如图 **54** 所示：

图表 54 添加探针第二步

3) 单击“完成”按钮，成功添加探针。如图 **55** 所示：

图表 55 添加探针第三步

注意：添加探针时，用户只用输入探针名称、探针 **IP** 和探针描述。关于探针的其他设置要在连接上探针且读出其相关设置后才能重新设置，即“修改探针”。

9.3 连接探针

步骤 1 在左边的分布式探针列表树视图中选中一个探针，然后将鼠标移到“探针管理”菜单，点击“连接探针”子菜单；如图 **56** 所示：

图表 56 连接探针子菜单

说明：

如果探针连接成功，探针左边的图标将由红色变为黄绿色，并且在信息栏中显示探针联接成功信息；如图 **57**、图 **58** 所示：

图表 57 探针联接成功时树视图状态

图表 58 探针联接成功时信息栏状态

9.4 断开探针

步骤 1 在左边的分布式探针列表树视图中点击一个探针，然后点击鼠标右键，在弹出式菜单中点击“断开探针”子菜单；如图 **59** 所示：

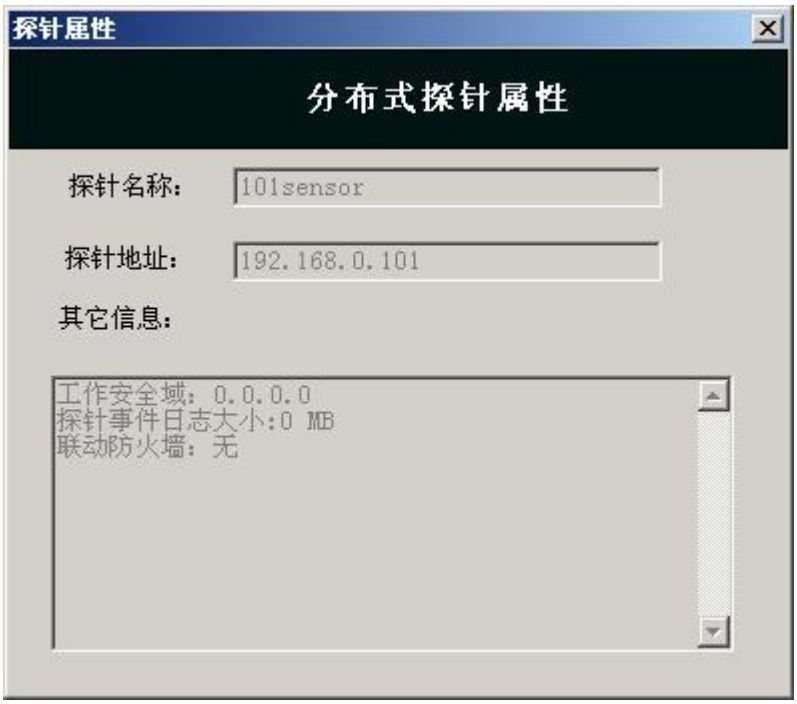
图表 59 树视图中的断开探针子菜单

9.5 探针属性

步骤 1 在左边的探针列表树视图中选中一个探针，然后点击鼠标右键，此时，将出现一个弹出式菜单，在弹出式菜单中点击“探针属性”子菜单；如图 **60** 所示；

图表 60 探针属性弹出式子菜单

步骤 2 系统将弹出一个对话框，来显示本探针的各项属性；如图 **61** 所示：



图表 61 探针属性对话框

9.6 修改探针

步骤 1 将鼠标移动到探针管理菜单上，点击“修改探针”子菜单；如图 **62** 所示：

图表 62 修改探针子菜单

或者在左边的探针列表中点击鼠标右键，在弹出式菜单中点击修改探针子菜单；如图 **63** 所示：

图表 63 树视图中的修改探针子菜单

步骤 2 此时，系统从探针处取出我们要修改探针的各个已经存在的参数，并初始化到探针设置的各个对话框中，本操步分为三小步：

1) 已经填写探针名称、探针地址和探针的简要描述等信息，如果想要更改探针的配置，直接修改就行了，填写完毕后，点击“下一步”按钮；如图 64 所示：

图表 64 修改探针第一步

2) 在策略设置界面中，有四个参数可以设置，探针安全域是设置我们要保护的网段的地址范围，记录探针事件日志是设置事件日志库的大小，而 **SYSLOG** 服务器是我们为联动提供的一个接口，在

这里只需要填写 SYSLOG 服务器的 IP 地址和相应的端口号即可。时钟同步是用来同步探针和控制台的时钟的，选中表示探针和控制台的时钟一致。填写完毕后，点击“下一步”按钮，如图 65 所示：

图表 65 修改探针第二步

3) 在下面出现的联动防火墙设置界面中，可以选择防火墙联动策略，IDS 系统支持的防火墙有三种，分别是北京天融信，NetScreen 3 .0，NetScreen 4 .0，对于不同的防火墙，它们的联动配置文件各有不同，选中它们中间一个，下面的配置选项相应的会要求输入。单击“完成”成功修改探针，所有修改的参数也将上传给探针，探针重启后立即生效。如图 66 所示：

图表 66 添加探针第三步

说明：

对于北京天融信防火墙，需要配置的是防火墙 IP 地址，联动时间，联动配置文件和联动密钥文件。其中联动配置文件和联动密钥文件是两个文件，在配置的时候只需要选中这两个文件即可。它们的所在的目录是安装目录下的"..\config\ FireWall\天融信"里面的两个文件，其中"key_file_IDS"是联动密钥文件，"topsec.conf"是联动配置文件；对于 NetScreen 3 .0 和 4.0 防火墙，它们要配置的是界面上看到的所有的配置项。其中，联动用户文件和联动密钥文件是在安装目录下的"..\config\ FireWall\\NetSreen"里面。"user.conf"是联动用户文件，"netscreen.key"是联动密钥文件。联动用户文件是可以编辑的，里面的用户名称就是 NetSreen 的用户名称。

完成修改探针以后，就要配置 **NetScreen** 防火墙了。

- **设置 NetScreen OS3.0，其步骤如下：**

1) 用 **Sshgen.exe** 产生 **public key** 和 **private key** 保存，注意产生的 **key** 类型为 **ssh1(rsa)** 保存 **private key** 时不需要密码；
2) 用 **console** 或 **telnet** 连接 **netscreen** 防火墙；
3) **set admin user mainer password 123456 privilege all** (注 **mainer** 表示一个新的用户)；
4) **set interface trust manage-ip 192.168.0.11**；
5) **set interface trust manage scs**；
6) **set scs enable**；
7) **set interface trust manage web**；
8) 设置 **pka-rsa**；
   set scs pka-rsa tftp username mainer file-name test20030422.pub ip-addr 192.168.0.100
   或用 **web** 设置；
9) **save**。

- **设置 NetScreen OS4.0，其步骤如下：**

1) 用 **Sshgen.exe** 产生 **public key** 和 **private key** 保存，注意产生的 **key** 类型为 **ssh1(rsa)** 保存 **private key** 时不需要密码；
2) 用 **console** 或 **telnet** 连接 **netscreen** 防火墙；
3) **set admin user mainer password 123456 privilege all** (注 **mainer** 表示一个新用户)；
4) **set interface vlan1 ip 192.168.0.1/24**；
5) **set interface trust manage scs**；
6) **set scs enable**；
7) **set interface trust manage web**；
8) 用 **web** 设置 **pka-rsa**；
9) **save**。

9.7 删除探针

步骤 1 在左边的探针列表中选中一个探针，点击鼠标右键，然后在弹出式菜单中点击“删除探针”子菜单项。如图 **67** 所示：

图表 67 删除探针子菜单

步骤 2 系统将弹出一个确认框，点击按钮 “是” 将删除本探针，否则，取消本次操作。如图 **68** 所示：

图表 68 删除探针确认

说明：

只有在探针处于断开状态是才可以删除，否则必须先断开连接然后再删除。

9.8 探针日志

步骤 1 将鼠标移动到探针管理菜单上，点击“探针日志”子菜单。探针日志就是下载从探针处的日志文件，在控制台这边，下载过来后，这个日志文件是存放在一个文本文件里面；如图 **69** 所示：

图表 69 探针日志子菜单

步骤 2 系统将弹出一个确认框，单击“确定”，将接受从探针处传过来的日志文件；如图 **70** 所示：

图表 70 探针日志确认

下载完成后，系统将用写字板打开它；如图 **71** 所示：

图表 71 日志显示在写字板上

9.9 查找探针

将鼠标移动到探针管理菜单上，点击“查找探针”子菜单，如图 **70**。查找探针是用来搜索探针的，它能够搜索到探针的 **IP** 地址，点击“探针搜索”，在 **30** 妙内，就能将探针的信息显示在 **List** 框里面。如图 **72** 所示：

图表 72 查找探针子菜单

9.10 升级探针

将鼠标移动到探针管理菜单上，点击“升级探针”子菜单。升级探针是由我们提供了探针升级包的情况下，对探针进行升级的一种方式，方法很简单，点击“升级探针”就会弹出一个对话框，选中升级包所在的路径，保存即可；如图 **73** 所示：

图表 73 升级探针子菜单

10. 策略管理

10.1 功能介绍

安全策略定制模块程序提供了通过图形化界面定制入侵行为检测和响应对的接口，使用户能够遵照菜单和按钮的引导，方便地定义企业统一安全策略所要求的入侵行为检测和响应对，并将定制的入侵行为检测和响应对列表，分发到各个分布式探针。模块提供添加、修改和删除等操作，易学易用。

模块同时提供良好的入侵行为规则自定义的图形界面，供用户定义新的入侵行为。自定义的入侵行为规则同样进入攻击特征数据库，供用户进行定制、选择，并分发给每个探针进行分析和检测。

安全策略定义入侵检测系统之分布式探针系统判断什么样的行为是入侵行为（检测），并对这种行为采取的什么样的相应对策（响应）。

具体来讲，用户依据使用权限可通过安全策略的各个子菜单，定制自己所需要的功能和策略。

10.2 策略管理

用户可以根据自身的要求进行策略的添加，策略的修改和策略的删除等操作来对安全策略进行管理。系统提供了专门的程序支持这一功能。

安全策略的定制过程涉及到两个窗口：

- 安全策略管理程序（窗口），管理具体的安全策略项；
- 安全策略编辑器，编辑每一个具体的安全策略项的内容。

10.2.1 接收策略

步骤 1 将鼠标移动到安全策略菜单上，点击“策略管理”子菜单；如图 **74** 所示：

图表 74 策略管理子菜单

步骤 2 系统将弹出一个策略管理界面，用户可以选择接收策略、新建策略、编辑策略、查看和删除策略操

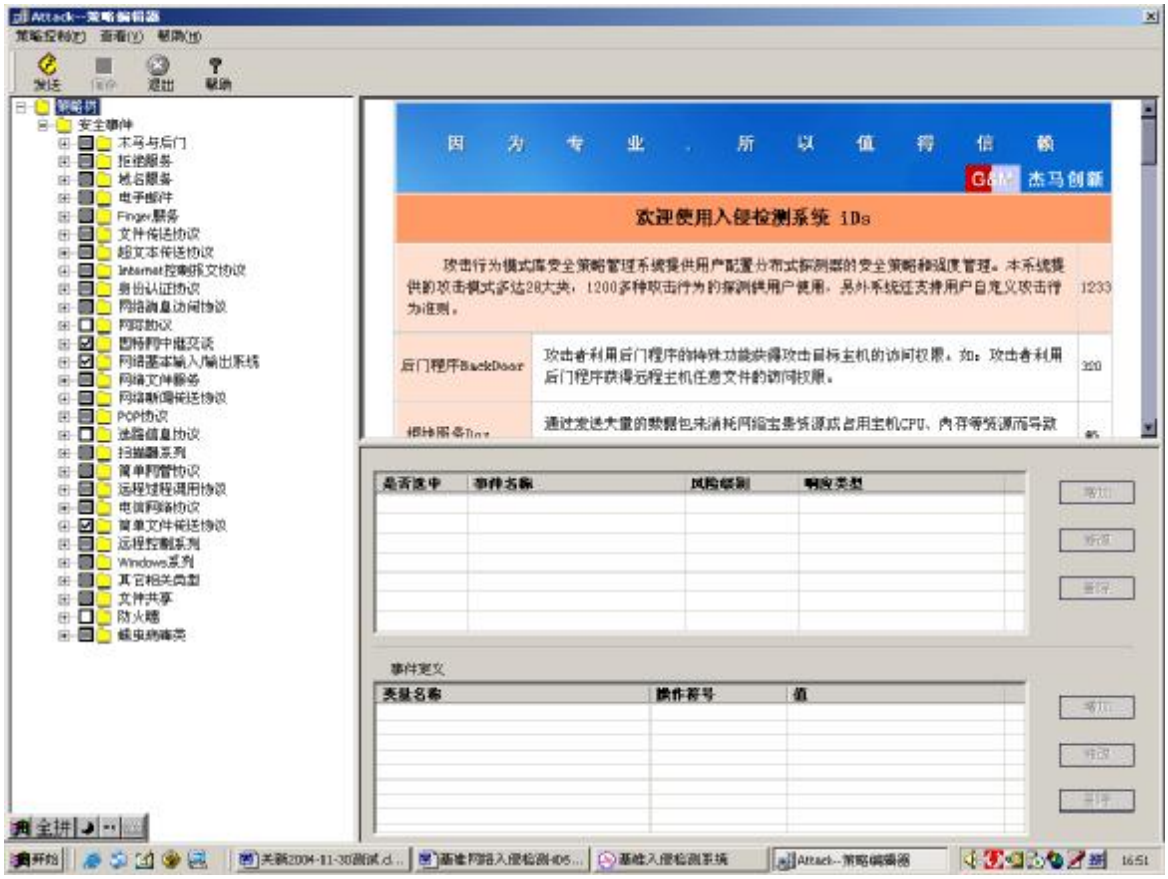
作，点击“选择从探针下载策略”选项，单击“接收策略”按钮，系统会接收正在工作的探针的策略；如图 **75** 所示：

图表 75 策略管理界面

弹出对话框提示策略已成功接收，单击“确定”；如图 **76** 所示：

图表 76 策略成功接收提示

进入探针策略编辑器；如图 **77** 所示：

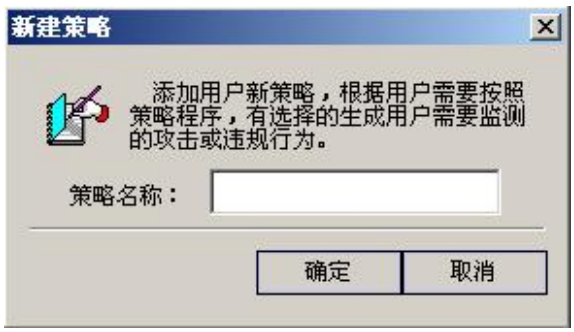


图表 77 探针策略编辑器

探针策略编辑器显示了本系统能够监测的所有的攻击（如图 **70** 左边的策略树）及其简要描述**(**如图 **70** 右上**)**，并且提供修改策略和添加新策略的编辑窗口（如图 **70** 右下）。本系统已经提供的攻击模式多达 **28** 大类，有 **1000** 多条攻击行为的探测供用户使用。关于新策略的生成和和旧策略的修改等的实现，下面会具体介绍。

10.2.2 新建策略

添加用户新策略，根据用户需要按照策略程序，有选择的生成用户需要监测的攻击或违规行为。策略管理允许用户根据自己的需要，新建安全策略。选择图 **68** 中的“选择编辑固有策略”选项，然后单击“新建策略”按钮，键入新策略名**,**最后按下“确定”按钮；如图 **78** 所示：



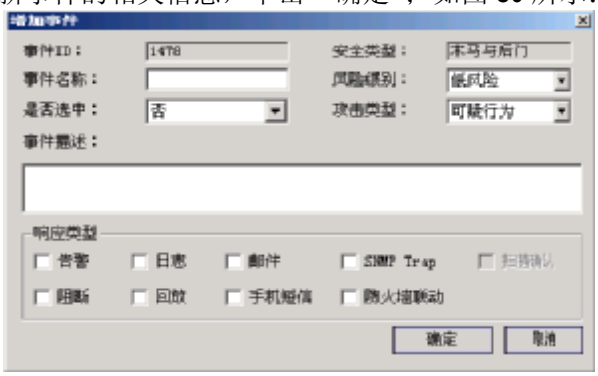
图表 78 新建策略

进入探针策略编辑器窗口，通过策略编辑器，可以对新建的策略进行编辑，自定义用户所需要的策略。自定义策略是用户根据自己的意志、愿望，依据用户对攻击行为的分析和理解，自行定义的一些攻击行为。这样就给用户带来了很大的自由度，提高了系统入侵检测的能力。策略定义（即新策略的编辑）的具体步骤如下：

步骤 1 在策略编辑器左边的策略树中选择要加入的新的攻击行为所属的大类。此时策略编辑器右下边的编辑框里会显示出该类攻击所包括的所有攻击事件，单击 “增加”按钮；如图 **79** 所示：

图表 79 网络基本输入/输出系统攻击

步骤 2 在弹出的对话框里输入新事件的相关信息，单击“确定”；如图 **80** 所示：



图表 80 新增事件的相关信息输入

步骤 3 选上新增事件，再单击下面的“增加”按钮，进行事件规则的编辑，完成规则定义后，单击“确认”按钮；如图 **81** 所示：

图表 81 事件规则定义

步骤 4 最后用户可以单击策略编辑器窗口（图 **70** 所示）的“保存”按钮，将新增事件保存并退出编辑器；或单击“发送”按钮，系统会根据用户需要选择将新增后的策略发送给当前的探针或指定 **IP** 地址的探针。

说明：

- 在事件信息输入和规则输入的过程中，可以利用“修改”和“删除”按钮作局部调整。
- 增加事件定义窗口里的“变量名”（即规则名）以及其代表的意义主要有：
  - **port** 服务所在的端口，如 **80**，默认只对发向此端口的包做匹配；
  - **alerted** 攻击模式的 **ID** 号；

这两项是必备的，下面的规则中必须有一项，否则会出现错误!!

  - **Act** 是反应，默认值 **0**，表示向控制台发消息；**1** 表示在 **SENSOR** 处作日志 （*）**4** 表示阻断连接；
  - **tos** 是 **IP** 报头的 **Type Of Service** 值；
  - **id** 是 **IP** 报头的 **ID** 值；
  - **ttl** 是 **IP** 报头的 **ttl** 值 ；
  - **fb** 是 **IP** 报头的 **fragbits** 和 **fargoffSET** 的值，**16** 位；
  - **len** 是 **TCP** 数据的长度，默认做大于判断
  - **start** 内容匹配的开始位置；
  - **end** 内容匹配的结束位置；
  - **flags** 包含 **6** 位 **TCP** 标志位和 **6** 位保留位，共 **12** 位有效，默认为对 **TCP6** 位作含有判断；
  - **spflag** 特殊标志位；

8	7	6	5	4	3	2	1

```
        |   |   |   |       |   |   |   |_____tcp flag （6 位）为相等判断
        |   |   |   |       |   |   |_________ tcp flag （6 位）为相反判断
        |   |   |   |   |       |_____________ 内容判断是使用大小写区分
          |   |   |   |   |_____________________ 对 flags 的 6 位保留位做等于判断
          |   |   |   |_________________________ 保留
          |   |   |_____________________________ 长度判断使用小于等于判断
          |   |_________________________________ 对从 port 发出和接收的数据报都匹配
          |_____________________________________对从 port 发出的数据报都匹配
```

  - **seq,ack TCP** 报头中的 **seq** 和 **ack** 值；
  - **cnt** ，**cnt2** 匹配的内容，可以是字符串，也可以是二进制序列；

- **msg** 附加消息，字符串；
- **option IP** 选项，未实现 。

10.2.3 编辑和查看策略

编辑策略是对已经存在的策略进行编辑，用户必须先选中策略表中的某一个策略，才能进入策略编辑器进行编辑。查看策略是只能查看某个策略的攻击行为的配置情况。不能进行编辑。这两个功能都要在策略编辑器里面完成。具体操作请参考新建策略的编辑策略部分。

10.2.4 上传和下载策略

下载策略是将当前探针的策略导出到硬盘中进行备份，在备份前用户可以做一些修改，修改后的策略可以保存也可以立即上传给当前探针。上传策略是将硬盘中存在的策略重新加载给当前探针。

（1） 下载策略

步骤 1 右击目标探针弹出下拉菜单，单击“策略下载”子菜单；如图 **82** 所示：

图表 82 探针下拉菜单

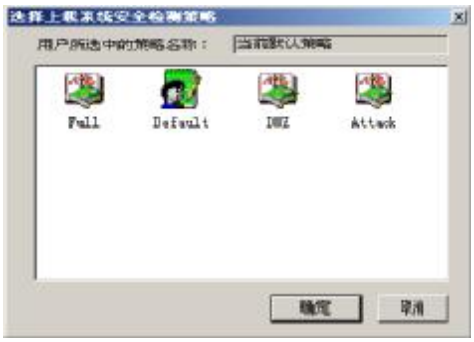
步骤 2 打开策略编辑器，用户可以在不做任何修改或修改后存盘，也可以通过“发送”快捷工具直接上传给当前探针或其他活动的探针。

（2） 上传策略

在图 **110** 的窗口中选择“策略上传”子菜单，系统弹出对话框，若单击“是”，系统会弹出固有策略选择对话框，若单击“否”按钮，系统会将探针的下载策略上传；如图 **83** 所示：

图表 83 策略上传确认对话框

在下面出现的固有策略选择对话框里选择一个策略，单击“确定”将策略上传给当前探针；如图 **84** 所示：



图表 84 上载策略选择对话框

10.2.5 删除策略

删除策略是提供给用户删除一些不必要的策略或者多余的策略的，先在如图 **83** 所示的策略列表中选中要删除的策略，然后点击“删除策略”按钮就可以删除该策略了。

10.3 规则过滤和地址绑定

规则过滤和地址绑定是提供给管理员自定义规则的。地址绑定是要求所在网络主机的 **MAC** 地址和 **IP** 地址不能改变，一旦有变化，就会产生告警。规则过滤是对于某种连接，我们认为是非法的，就应该禁止，将其过滤掉。一旦产生这个连接，系统告警。

10.3.1 进入地址过滤

步骤 1 将鼠标移动到安全策略菜单上，点击“地址过滤”子菜单；如图 **85** 所示：

图表 85 地址过滤子菜单

步骤 2 本系统将弹出一个规则过滤和地址绑定界面；如图 **86** 所示：

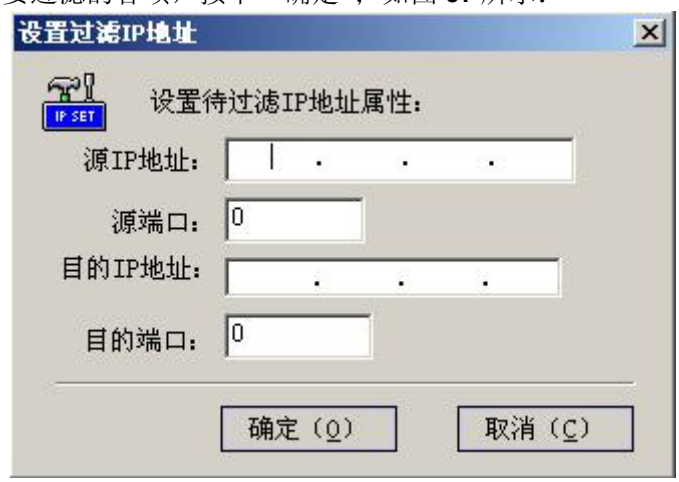
图表 86 规则过滤和地址绑定

10.3.2 规则过滤和地址绑定的功能描述

规则过滤和地址绑定（图 **79**）是由两个属性页组成的，对于每个单独的属性页，都有“添加”和“删除”功能。

- **IP** 地址和端口过滤的添加功能

添加一个过滤地址，对于管理员来说是必要的，在“**IP** 地址和地址过滤”标签下单击“增加”出现下面对话框，用户输入想要过滤的各项，按下“确定”；如图 **87** 所示：



图表 87 设置过滤 IP 地址

说明：

在图 **87** 中的列表框中会显示加入的这一项。这里的各个项目是可以为空的，置为空表示任意的端口或 **IP** 地址。

- **IP** 地址和端口过滤的删除功能

在列表框中选中要删除的项，单击“删除”即可完成；如图 **88** 所示：

图表 88 选中删除 IP 项

说明：

完成删除后，该项也会从列表框中被删除。

- **IP** 地址和 **MAC** 绑定的添加功能

在规则过滤和地址（图 **87**）中，切换到 **IP** 地址和 **MAC** 绑定属性页，单击“添加”，出现下面的对话框，填写相应的 **IP** 和 **MAC** 地址，单击“确定”；如图 **89** 所示：

图表 89 绑定 MAC 地址和 IP 地址窗体

说明：

在图 **87** 中的 **IP** 地址和 **MAC** 绑定属性页的列表框中会显示加入的这一项。

- **IP** 地址和 **MAC** 绑定的删除功能

在列表框中选中要删除的项，单击“删除”即可完成。如图 **90** 所示：

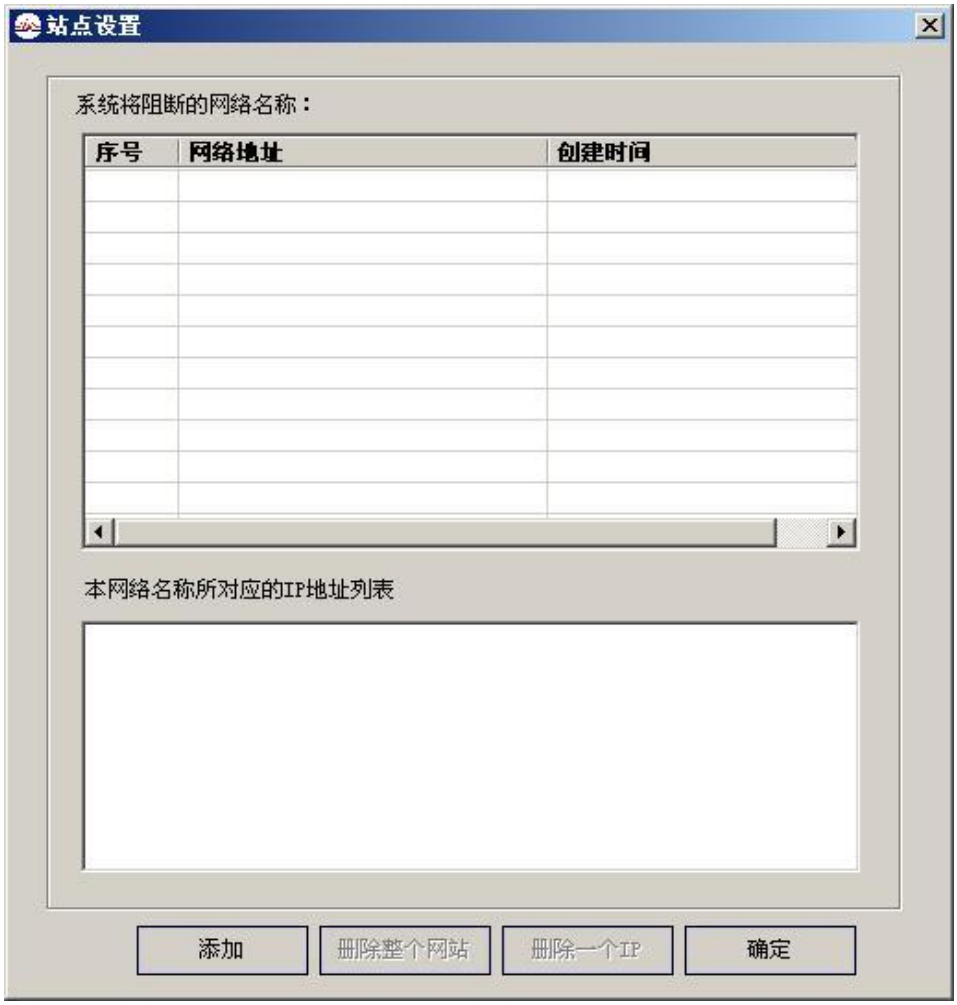
图表 90 选中删除项

说明：

操作完成后，点击“退出”回到主控制台。

10.4 禁用黑名单

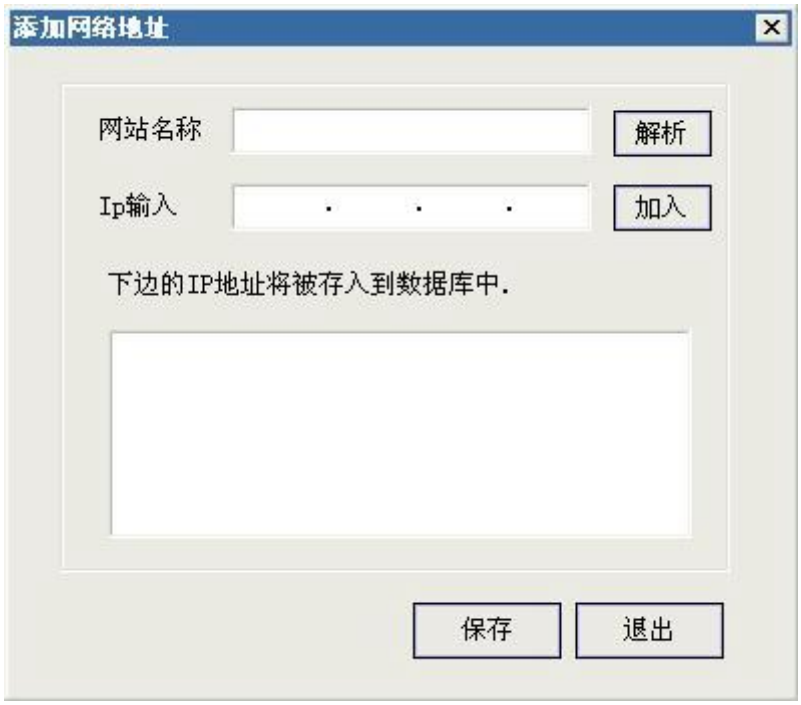
使用禁用黑名单，通过设置我们可以阻断某些网络，它提供添加和删除黑名单的功能；如图 **91** 所示：



图表 91 禁用黑名单主界面

10.4.1 添加功能

在图 92 中，点击“添加”按钮出现 IP 网络地址对话框，输入其中的各项数据，点击“保存”按钮成功添加；如图 92 所示：



图表 92 添加黑名单

10.4.2 删除功能

在图 92 中，有两个按钮——“删除整个网站”和“删除一个 IP”。由于有很多的网站都拥有很多的 IP 地址，删除整个网站，就是要删除网站及其拥有的所有的 IP 地址，删除一个 IP 就是删除某网站拥有的众多 IP 中的一个 IP。当然，无论是删除整个网站还是删除一个 IP，首先都要选中它，然后单击相应的按钮。

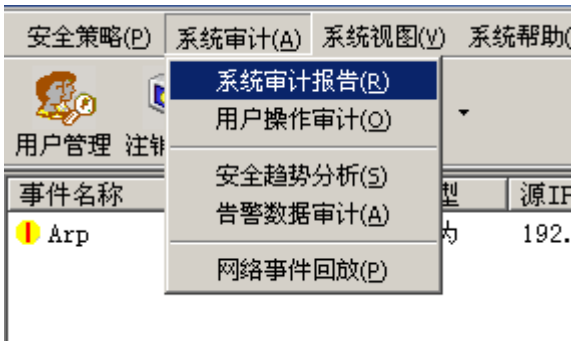
11. 系统审计

11.1 功能介绍

系统审计对本系统的一些告警事件、回放事件、日志等数据进行综合和分析，得到一些可用信息。

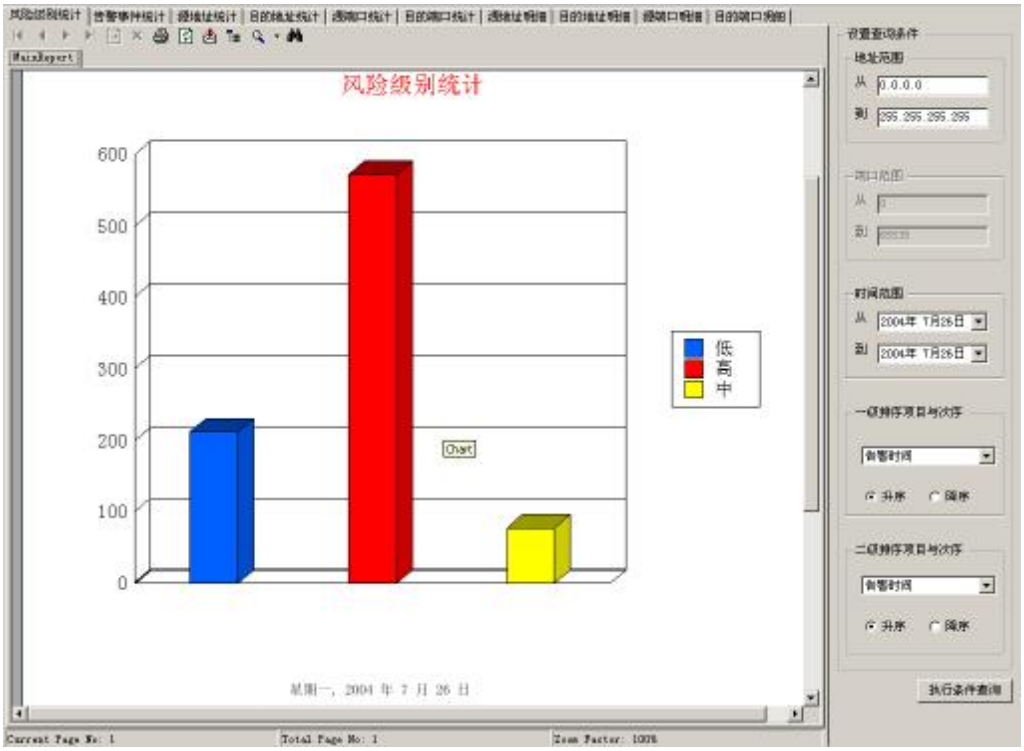
11.2 系统告警报告

步骤 1 将鼠标移动到系统审计菜单上，点击“系统审计”报告子菜单；如图 **93** 所示：



图表 93 系统审计报告子菜单

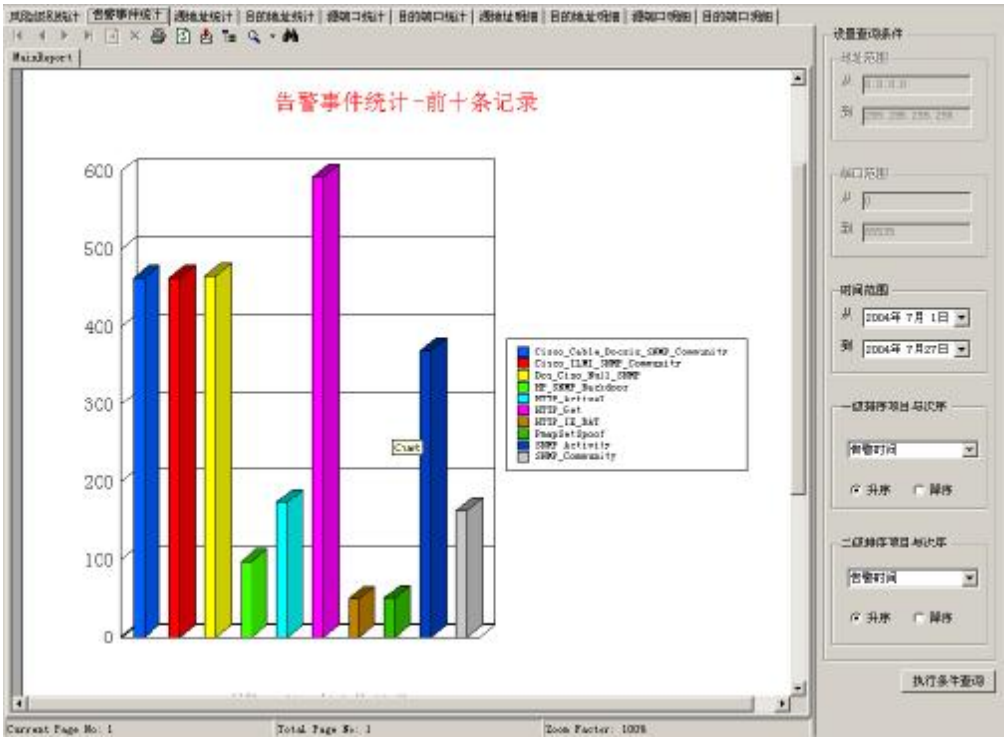
步骤 2 出现报告显示界面；如图 **94** 所示：



图表 94 报告显示界面

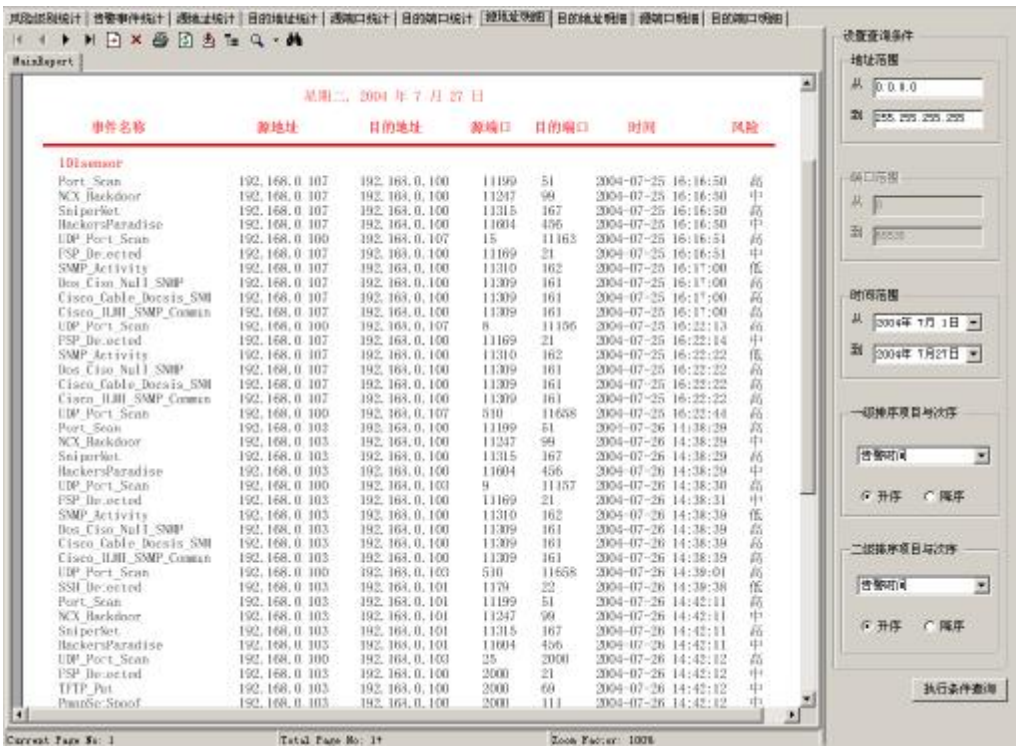
步骤 3 在报告显示界面（图 **87**）中可根据需要进行参数设置。选定所需报表，点击执行查询条件。例

如：点击“报警事件统计”，再点击执行查询条件结果；如图 **95** 所示：



图表 95 报表查询

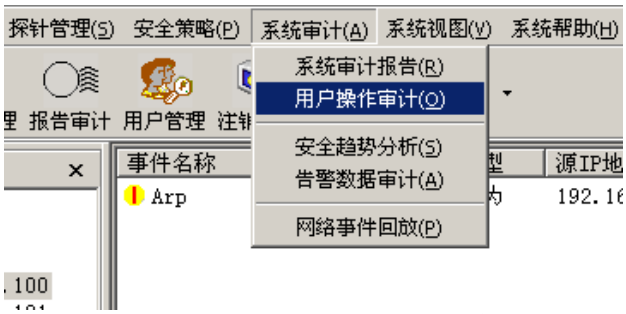
点击“源地址明细报表”；再点击执行查询条件结果；如图 **96** 所示：



图表 96 源地址明细报表

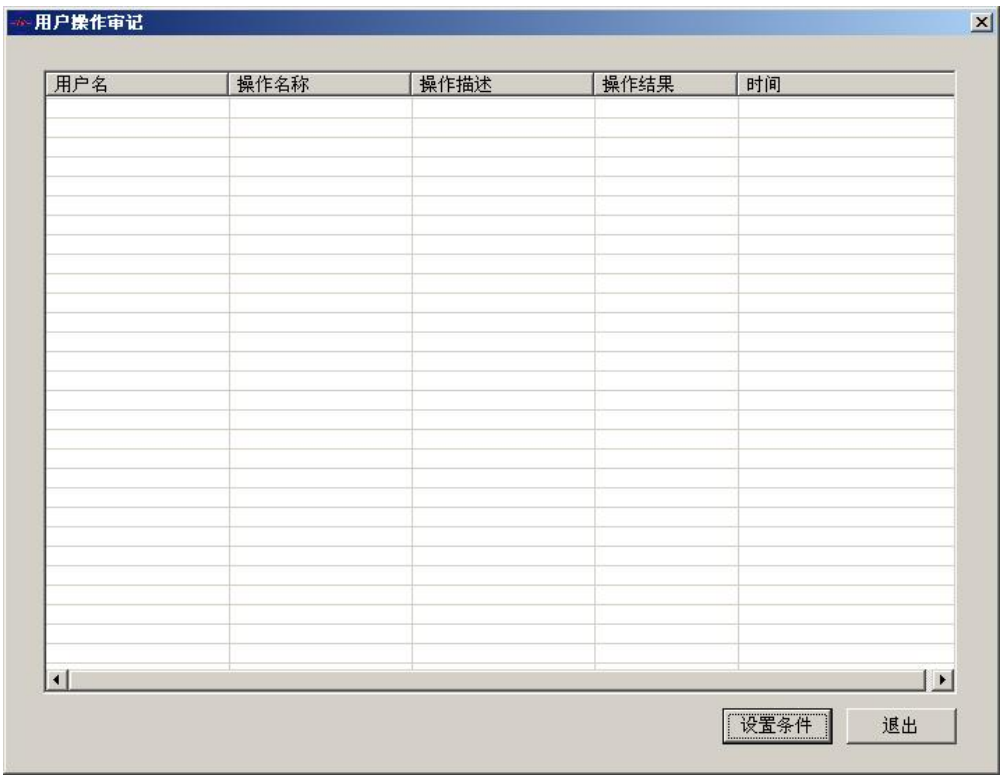
11.3 用户操作审计

用户操作审计是对用户操作控制台的行为进行审计，将鼠标移动到系统审计菜单上，点击“用户操作审计”子菜单；如图 **97** 所示：



图表 97 用户操作审计子菜单

弹出下面出现的用户操作审计窗口，如图 **98** 所示：



图表 98 用户操作审计界面

用户可以通过设置条件，具体来说是通过设置时间段，来设置感兴趣的或者需要的信息，设置好时间段后，点击“确定”按钮；如图 **99** 所示：

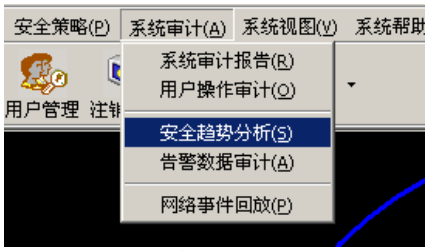
图表 99 设置查询条件

说明：

在用户操作审计界面（图 **89**）中，点击“开始查询”按钮，就可以在列表框中显示出用户的所有操作。

11.4 安全趋势分析

步骤 1 安全趋势分析是对一定时间段内的安全状况进行统计分析，给出网络系统在未来的一段时间内的安全状况走势。将鼠标移动到“系统审计”菜单上，出现“安全趋势分析”子菜单；如图 **100** 所示：



图表 100 安全趋势分析子菜单

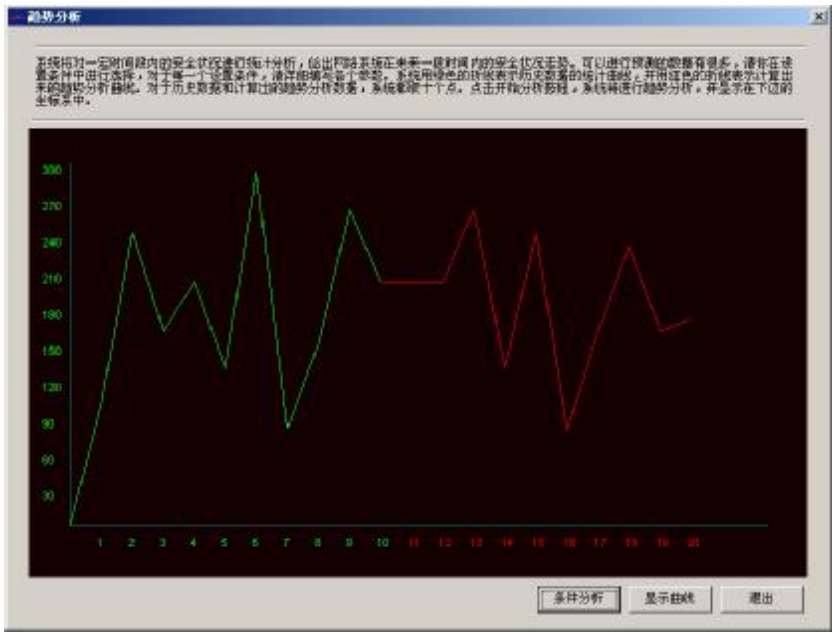
步骤 2 点击系统“安全趋势分析”子菜单，出现条件设置窗口，安全趋势分析可以进行预测的数据是很多的，用户可以在条件分析中进行选择，对于每个条件，都要设置具体一点根据窗口里面的提示，设置完成后，点击“分析”，如图 **101** 所示：

图表 101 设置条件

如果条件合适，将会弹出一个对话框；如图 **102** 所示：

图表 102 显示趋势分析成功

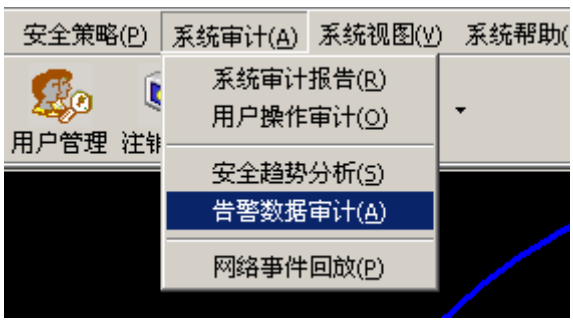
点击“显示曲线”按钮就可以查看分析结果，在此曲线中，绿色的曲线代表是历史数据，而红色的曲线是代表的是计算出来的趋势分析曲线。就是一个趋势分析成功的曲线；如图 **103** 所示：



图表 103 一个趋势分析实例

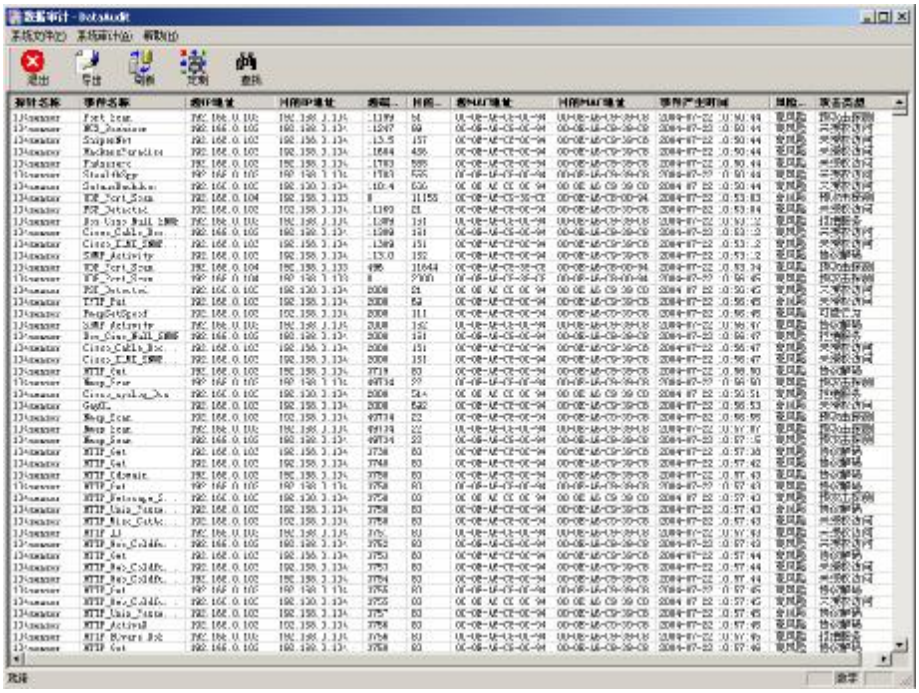
11.5 告警数据审计

步骤 1 将鼠标移动到系统审计菜单上；如图 **104** 所示：



图表 104 告警数据审计子菜单

步骤 2 点击“告警数据审计”子菜单，进入其主菜单，如图 **105** 所示：



图表 105 数据审计主界面

说明：

在数据审计中主要提供了两个功能，即查找和定制。在打开该主界面的时候，显示的数据是所有的告警数据。在这么多的数据中，如何找到用户感兴趣的数据呢？可以通过定制和查找来实现。

步骤 3 在工具栏里直接点击“定制”，或者在系统审计菜单中点击“定制窗口”子菜单，都可以进入定制窗口主界面，在列表框中选择需要的项，点击“确定”按钮；如图 **106** 所示：

图表 106 定制窗口界面

说明：

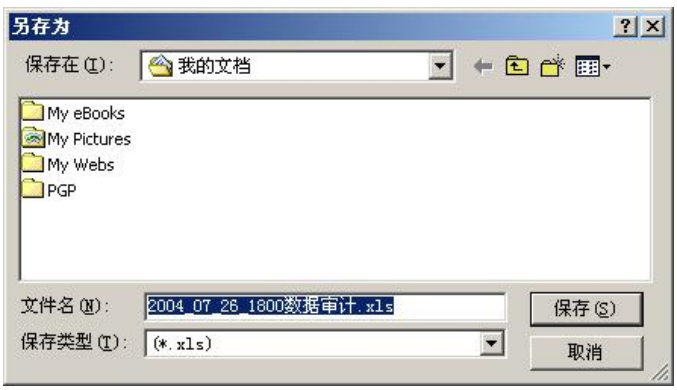
- 同时在主界面中，也已经显示了定制的数据。
- 当然，也可以通过查找来定制窗口界面，在工具栏里直接点击“查找”，或者在系统审计菜单中点击“数据查询”子菜单，都可以进入定制窗口主界面。如图 **107** 所示：

图表 107 数据查询参数

在这个窗体中，有三种参数可以定制，分别是地址参数、时间参数、其他参数。地址参数是通过 **IP** 地址进行定制，时间参数是定制告警事件的时间段，其他参数有源端口和目的端口，还有告警事件的名称。

根据需要，配置完这些参数后，点击“查询”按钮即可。同时在主界面中，也已经显示了定制的数据。

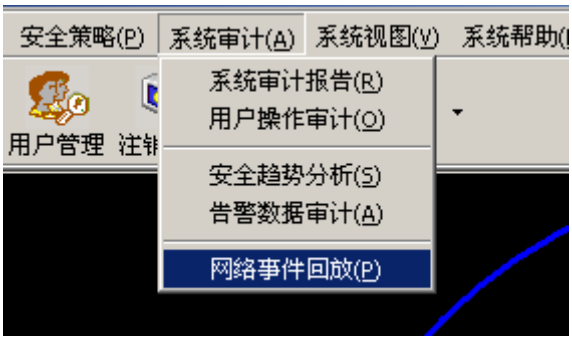
将定制窗口和数据查询结合起来使用，会很好的定制用户所需要的记录。定制完成后，还可以将定制的结果导出存盘。在工具栏里直接点击“导出”，或者在系统文件菜单中点击“导出”子菜单，就会弹出一个对话框，单击“保存”按钮，该定制就被保存了。其保存的数据格式是 **Excel**，扩展名是 **xls**。；如图 **108** 所示：



图表 108 导出数据审计

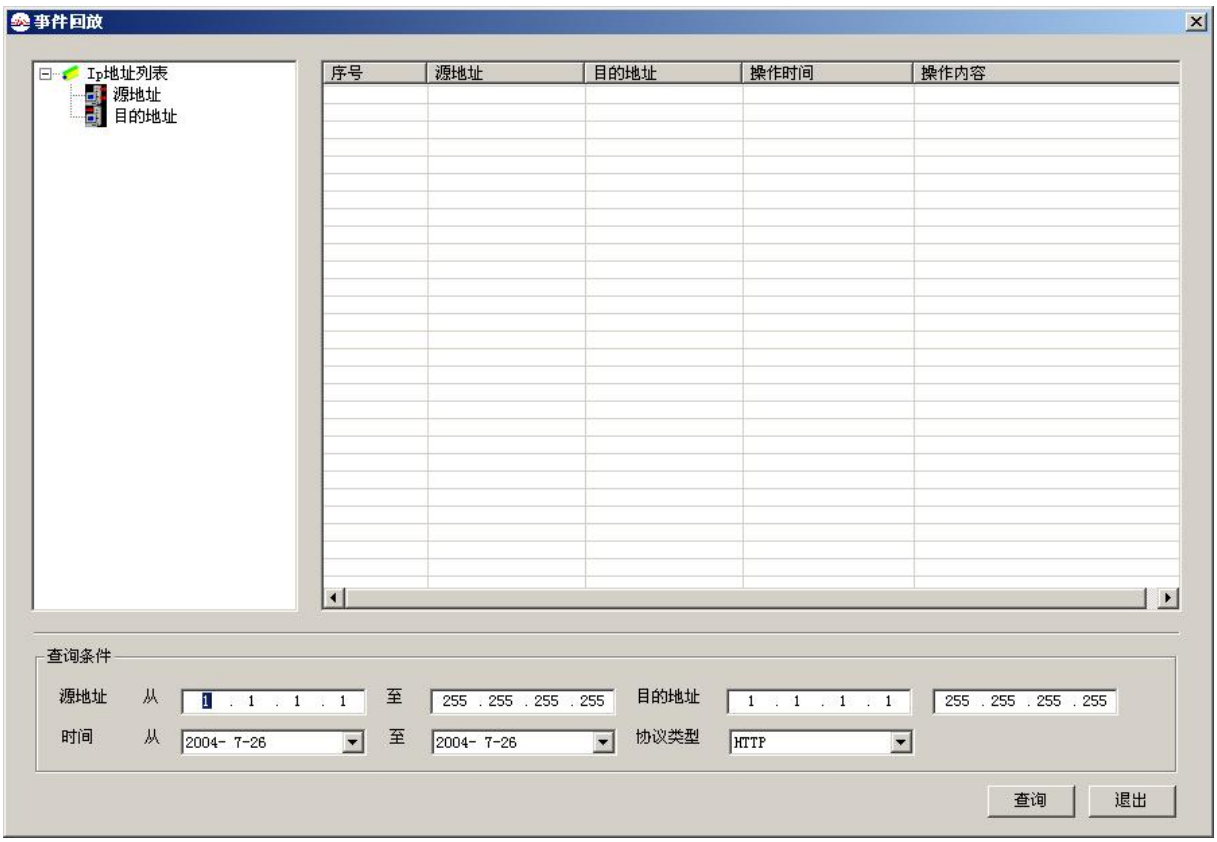
11.6 网络事件回放

将鼠标移动到系统审计菜单上，如图 **109** 所示：



图表 109 网络事件回放子菜单

单击“网络事件回放”子菜单，系统弹出网络事件回放主界面，用户可以输入如：源地址、目的地址、协议类型等条件，然后单击“查询”按钮，实现历史事件的回放；如图 **110** 所示：



图表 110 网络事件回放

12. 系统帮助

12.1 功能介绍

基准入侵检测系统提供了强大的帮助系统。用户可以在菜单中和工具栏中点击“系统帮助”，就可以轻松进入帮助信息。帮助信息包括：查阅系统帮助；网上 IDS；IDS 在线升级以及 IDS 版本信息。

12.2 进入系统帮助

用户可以在“系统帮助”菜单中点击“IDS 帮助”或工具栏中点击“系统帮助”，就可以轻松进入帮助信息。用户可以查看本说明书，检索相关内容，获取帮助。如图 111、图 112 所示：

图表 111 系统帮助菜单

图表 112 系统帮助

12.3 网上IDS系统

用户可以在“系统帮助”菜单中点击“网上 IDS”，就可以获得网上系统最新信息。

12.4 系统在线升级

如果用户接入了 **Internet** 网，单击“系统帮助”菜单的“**IDS** 在线升级”子菜单，如图，进入在线升级相关信息设置对话框。如图 **114** 所示：

图表 114 在线升级

12.5 系统版本信息

单击“系统帮助”菜单的“关于 **IDS**”子菜单，进入系统版本信息对话框。如图 **115** 所示：

图表 115 系统版本信息

13. 疑难解答 FAQs

什么是基准入侵检测系统？
基准入侵检测系统是实时网络自动违规识别和响应系统，是一种实时的、自动的网络入侵与违规行为识别、网络攻击情报预警和对入侵行为与征兆的响应系统。
使用基准入侵检测系统会对网络性能产生影响么？
不会的，入侵检测系统属于网络旁路设备，采用监听得方式侦测网络数据，不会对网络性能造成任何影响。
基准入侵检测系统支持什么样的网络环境？
支持 10m/100m/1000m 的以太网环境，通过共享式网络设备或交换机镜像口接入网络，由于采用分布式结构，用户可以灵活选择探针的安置，在需要的网段安置探针而通过集中管理端进行统一管理。
我已经完成探针的安置和控制台的安装，为什么不能启动控制台？
控制台除了主程序得安装还需要 SQL Server ，.NET 框架 等程序的支持，请耐心按照安装手册提示完成安装。
为什么我得控制台没有任何数据显示？
² 请检查控制台能否正常与探针连接，或是否选择连接探针。 ² 探针是否连接在共享式网络设备上，或者交换机镜像是否正常工作。 ² 网络状况良好，没有任何入侵事件。
第一次使用时为什么系统提示授权有误？
请您拷贝光盘中的 IDS.Key 文件到安装目录，在菜单中选择系统维护－>系统授权－>浏览 选择授权文件确定以添加授权（系统默认的授权是三个月的全址：0.0.0.0/255.255.255.255—出厂之日开始算，请您再购买后以 E-mail 或电话方式告知您的 ip 地址范围。也可在您购买时提供 ip 地址范围，以便授权。由此给您带来的不便，我公司表示歉意！）
我怎么知道探针的 ip 地址？
² 探针默认的初始ip地址为192.168.0.1 您可以通过控制台（console）来修改探针（sensor-黑匣子）的IP地址，方法详见第60页； ² 如果您修改了探针地址而又忘记了，您可以选择菜单项 探针管理－》查找探针来查找网络中存在的探针。
配置完 SQL 之后启动控制台时会提示找不到数据源？
² 请确认数据库已附加完成； ² 请严格按照安装手册上所写的步骤来配置ODBC；
报表功能无法使用
请确定已安装 .NET 框架等其它支持程序。（如果没有安装，请安装/program files/gminnova/IDS/console/reportsupport 下的文件）
系统使用是否安全？
探针和控制台通信使用了加密的通信协议，保证数据不会被截取或破坏，探针的监听口没有 ip 地址，很难被网络上其它设备发现。可以说入侵检测系统是非常安全的。